



“十二五”职业教育国家规划教材
经全国职业教育教材审定委员会审定

网络设备安装与调试 (思科版)

陈 颜 门雅范 张文库 主 编
代树强 楚 扬 李凤丽 副主编



电子工业出版社

Publishing House of Electronics Industry

北京 • BEIJING

VISIT...

LANZAROTE
Caliente.COM

内 容 简 介

本书根据教育部颁发的《中等职业学校专业教学标准（试行）信息技术类（第一辑）》中的相关教学内容和要求编写。本书的编写从满足经济发展对高素质劳动者和技能型人才的需求出发，在课程结构、教学内容、教学方法等方面进行了新的探索与改革创新，以利于学生更好地掌握本课程的内容，利于学生理论知识的掌握和实际操作技能的提高。

本书以知识“必需、够用”为原则，从职业岗位分析入手展开教学内容，强化学生的技能训练和职业能力，在训练中巩固所学知识。从 Cisco 公司的 Packet Tracer 使用开始，通过模拟器的使用，交换技术基础、路由技术基础、路由协议实现、广域网技术实现等项目完成技能训练，通过网络安全技术实现、防火墙技术实现完成网络安全技能训练，通过无线网络技术的实现完成无线技术的技能训练，最后以企业、公司网络综合实训结束整个网络综合技能训练。

本书可作为计算机网络技术专业一体化教材，也可以作为相关培训教材，还可作为计算机网络技能比赛训练及广大网络工程技术人员的技术参考书。本书配有教学指南、电子教案和完整配置代码，详见前言。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有，侵权必究。

图书在版编目（CIP）数据

网络设备安装与调试：思科版/陈颜，门雅范，张文库主编. —北京：电子工业出版社，2018.3

“十二五”职业教育国家规划教材 经全国职业教育教材审定委员会审定

ISBN 978-7-121-29286-6

I. ①网… II. ①陈… ②门… ③张… III. ①网络设备—设备安装—中等专业学校—教材
②网络设备—调试方法—中等专业学校—教材 IV. ①TP393

中国版本图书馆 CIP 数据核字（2016）第 152059 号

策划编辑：杨 波

责任编辑：裴 杰

印 刷：

装 订：

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

开 本：787×1 092 1/16 印张：17.5 字数：448 千字

版 次：2018 年 3 月第 1 版

印 次：2018 年 3 月第 1 次印刷

定 价：38.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888，88258888。

质量投诉请发邮件至 zltz@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

本书咨询联系方式：（010）88254584。

编审委员会名单

主任委员：

武马群

副主任委员：

王 健 韩立凡 何文生

委 员：

丁文慧	丁爱萍	于志博	马广月	马之云	马永芳	马玥桓	王 帅	王 蓓
王 彬	王晓姝	王家青	王皓轩	王新萍	方 伟	方松林	孔祥华	龙天才
龙凯明	卢华东	由相宁	史宪美	史晓云	冯理明	冯雪燕	毕建伟	朱文娟
朱海波	向 华	刘 凌	刘小华	刘天真	关 莹	江永春	许昭霞	孙宏仪
苏曰太夫	杜 珺	杜宏志	杜秋磊	李 飞	李 娜	李华平	李宇鹏	杨 杰
杨 怡	杨春红	吴 伦	何 琳	余运祥	邹贵财	沈大林	宋 微	张 平
张 侨	张 玲	张士忠	张文库	张东义	张兴华	张呈江	张建文	张凌杰
张媛媛	陆 沁	陈 玲	陈 颜	陈丁君	陈天翔	陈观诚	陈佳玉	陈泓吉
陈学平	陈道斌	范铭慧	罗 丹	周 鹤	周海峰	庞 震	赵艳莉	赵晨阳
赵增敏	郝俊华	胡 尹	钟 勤	段 欣	段 标	姜全生	钱 峰	徐 宁
徐 兵	高 强	高 静	郭 荔	郭立红	郭朝勇	涂铁军	黄 彦	黄汉军
黄洪杰	崔长华	崔建成	梁 姍	彭仲昆	葛艳玲	董新春	韩雪涛	韩新洲
曾平驿	曾祥民	温 晞	谢世森	赖福生	谭建伟	戴建耘	魏茂林	

序 | PROLOGUE

当今是一个信息技术主宰的时代，以计算机应用为核心的信息技术已经渗透到人类活动的各个领域，彻底改变着人类传统的生产、工作、学习、交往、生活和思维方式。和语言和数学等能力一样，信息技术应用能力也已成为人们必须掌握的、最为重要的基本能力。职业教育作为国民教育体系和人力资源开发的重要组成部分，信息技术应用能力和计算机相关专业领域专项应用能力的培养，始终是职业教育培养多样化人才、传承技术技能、促进就业创业的重要载体和主要内容。

信息技术的发展，特别是数字媒体、互联网、移动通信等技术的普及应用，使信息技术的应用形态和领域都发生了重大的变化。第一，计算机技术的使用扩展至前所未有的程度，桌面电脑和移动终端（智能手机、平板电脑等）的普及，网络和移动通信技术的发展，使信息的获取、呈现与处理无处不在，人类社会生产、生活的诸多领域已无法脱离信息技术的支持而独立进行；第二，信息媒体处理的数字化衍生出新的信息技术应用领域，如数字影像、计算机平面设计、计算机动漫游戏、虚拟现实等。第三，信息技术与其他业务的应用有机结合，如与商业、金融、交通、物流、加工制造、工业设计、广告传媒、影视娱乐等结合，形成了一些独立的生态体系，综合信息处理、数据分析、智能控制、媒体创意、网络传播等日益成为当前信息技术的主要应用领域，并诞生了云计算、物联网、大数据、3D 打印等指引未来信息技术应用的发展方向。

信息技术的不断推陈出新及应用领域的综合化和普及化，直接影响着技术、技能型人才的培养定位，并引领着职业教育领域信息技术或计算机相关专业与课程改革、配套教材的建设，使之不断推陈出新、与时俱进。

2009 年，教育部颁布了《中等职业学校计算机应用基础大纲》；2014 年，教育部在 2010 年新修订的专业目录基础上，相继颁布了“计算机应用、数字媒体技术应用、计算机平面设计、计算机动漫与游戏制作、计算机网络技术、网站建设与管理、软件与信息服务、客户信息服务、计算机速录”等 9 个信息技术类相关专业的教学标准，确定了教学实施及核心课程内容的指导意见。本书就是以此为依据，结合当前最新的信息技术发展趋势和企业应用案例组织开发和编写的。



本套系列教材的主要特色

● 对计算机专业类相关课程的教学内容进行重新整合

本套教材面向学生的基础应用能力，设定了系统操作、文档编辑、网络使用、数据分析、媒体处理、信息交互、外设与移动设备应用、系统维护维修、综合业务运用等内容；针对专业应用能力，根据专业和职业能力方向的不同，结合企业的具体应用业务规划了教材内容。

● 以岗位工作过程来确定学习任务和目标，综合提升学生的专业能力、过程能力和职位差异能力

本套教材通过工作过程为导向的教学模式和模块化的知识能力整合结构，体现产业需求与专业设置、职业标准与课程内容、生产过程与教学过程、职业资格证书与学历证书、终身学习与职业教育的“五对接”。在学习目标到内容的设计上，本套教材不再仅仅是专业理论内容的复制，而是经由职业岗位实践——工作过程与岗位能力分析—技能知识学习应用内化的学习实训导引和案例。借助知识的重组与技能的强化，达到企业岗位情境和教学内容要求相贯通的课程融合目标。

● 以项目教学和任务案例实训作为主线

本套教材通过项目教学，构建了工作业务的完整流程和岗位能力需求体系。项目的确定应遵循 3 个基本目标：核心能力的熟练程度、技术更新与延伸的再学习能力、不同业务情境应用的适应性。教材借助以校企合作为基础的实训任务，以应用能力为核心、以案例为线索，通过设立情境、任务解析、引导示范、基础练习、难点解析与知识延伸、能力提升训练和总结评价等环节引领学者在任务的完成过程中积累技能、学习知识，并迁移到不同业务情境的任务解决过程中，使学者在未来可以从容面对不同应用场景的工作岗位。

当前，全国职业教育领域都在深入贯彻全国工作会议精神，学习领会中央领导对职业教育的重要批示，全力加快推进现代职业教育。国务院出台的《加快发展现代职业教育的决定》明确提出要“形成适应发展需求、产教深度融合、中职高职衔接、职业教育与普通教育相互沟通，体现终身教育理念，具有中国特色、世界水平的现代职业教育体系”。现代职业教育体系的建立将带来人才培养模式、教育教学方式和办学体制机制的巨大变革，这无疑给职业院校信息技术应用人才培养提出了新的目标。计算机类相关专业的教学必须适应改革，始终把握技术发展和技术技能人才培养的最新动向，坚持产教融合、校企合作、工学结合、知行合一，为培养出更多适应产业升级转型和经济发展的高素质职业人才做出更大贡献！

前言 | PREFACE

为建立健全教育质量保障体系，提高职业教育质量，教育部于 2014 年颁布了《中等职业学校专业教学标准》（以下简称《专业教学标准》）。《专业教学标准》是指导和管理中等职业学校教学工作的主要依据，是保证教育教学质量和人才培养规格的纲领性教学文件。在“教育部办公厅关于公布首批《中等职业学校专业教学标准（试行）》目录的通知”（教职成厅[2014]11 号文）中，强调“专业教学标准是开展专业教学的基本文件，是明确培养目标和规格、组织实施教学、规范教学管理、加强专业建设、开发教材和学习资源的基本依据，是评估教育教学质量的主要标尺，同时也是社会用人单位选用中等职业学校毕业生的重要参考。”计算机网络技术专业的职业范围见下表。

1. 本书特色

本书根据教育部颁发的《中等职业学校专业教学标准（试行）信息技术类（第一辑）》中的相关教学内容和要求编写。

本书总结了编者多年来计算机网络工程实践及教学的经验，根据网络工程实际工作过程所需要的知识技能提炼出若干个教学项目。全书先提出学习情境，再提供完成该情境所必须掌握的操作技能及相关理论知识，部分项目还有知识拓展，供有余力的学生课外学习，同时安排了学习小结，供学生对本活动知识点进行总结，在项目的最后安排了项目考核，供学生课后练习。每个项目以要实现的实训为核心来组织，实训中又细分为任务，形成了“项目—实训—任务”的结构体系，通过一个个任务使学生掌握相关知识和技能。每个任务基本上细分为“学习情境—情境分析—步骤实现—相关知识—学习小结”等版块，从工作现场需求与实践应用中引入教学项目，培养学生完成工作任务而需要掌握的技能。

整个课程根据内容共分为多个任务，每个任务严格遵循网络工程施工流程设计，侧重规划设计与网络设备具体功能实现的编写。

通过对本课程的学习，使学生了解 Cisco 公司的 Packet Trace 软件的使用，了解 Cisco 交换机、路由器、无线 AP 和防火墙的功能，熟练掌握交换技术的 VLAN 技术、STP 技术、VTP 技术和三层交换等相关技术，熟练掌握路由技术的单臂路由、静态路由协议和动态路由协议等技术，熟练无线 AP 和防火墙的基本功能和技术。

2. 课时分配

本书参考学时为 96 学时，具体分配见本书配套的电子教案。



3. 教学资源

为了提高学习效率和教学效果，方便教师教学，作者为本书配备包括了电子教案、教学指南、完整配置代码，以及习题参考答案等配套的教学资源。请有此需要的读者登录华信教育资源网（<http://www.hxedu.com.cn>）免费注册后进行下载，有问题时请在网站留言板留言或与电子工业出版社联系（E-mail:hxedu@phei.com.cn）。

4. 本书编者

本书由陈颜、门雅范和张文库担任主编并负责统稿，代树强、楚扬和李凤丽担任副主编。本书具体编写分工如下：庄云娟、祝捷负责编写项目 1，门雅范负责编写项目 2，代树强、周鹏负责编写项目 3，楚扬、赵亮负责编写项目 4，陈颜负责编写项目 5，陈韦华负责编写项目 6，张文库负责编写项目 7，邓宁负责编写项目 8，李凤丽、王皓宇负责编写项目 9。

由于编者水平有限，加之时间有限，书中难免有错误和不妥之处，恳请广大师生和读者批评指正。

编 者

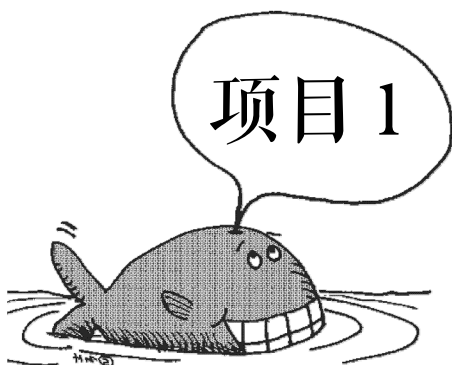
CONTENTS | 目录



项目1 Cisco Packet Tracer 6.1	
Instructor模拟器的使用	1
实训1 安装 Cisco Packet Tracer	
6.1 Instructor 模拟器	2
实训2 使用 Cisco Packet Tracer6.1	
Instructor 搭建网络	8
项目2 交换技术基础	13
实训1 交换机的基本配置	14
任务1 交换机的几种配置	
模式	14
任务2 交换机的基本配置	19
任务3 交换机的配置文件	
管理	23
任务4 交换机系统的备份与	
升级	28
任务5 交换机的 Telnet 配置	31
实训2 交换机的 VLAN 配置	36
任务1 交换机的 VLAN 划分	37
任务2 交换机间相同 VLAN	
通信	41
任务3 三层交换机的配置	47
实训3 交换机的常用技术	50
任务1 交换机的链路聚合	
技术	51
任务2 交换机的 VTP 技术	55
任务3 交换机的 STP 技术	60
任务4 交换机的 DHCP 技术	65
任务5 交换机的 HSRP 技术	69
项目3 路由技术基础	76
实训1 路由器的设置	77
实训2 路由器的基本配置	81
实训3 单臂路由的配置	87
实训4 路由器系统的备份与恢复	89
实训5 路由器的 DHCP 配置	95
实训6 路由器的 Telnet 配置	97
项目4 路由协议实现	105
实训1 静态路由配置	106
实训2 动态路由配置	119
任务1 RIP 动态路由配置	119
任务2 EIGRP 动态路由配置	132
任务3 OSPF 动态路由配置	143
项目5 网络安全技术实现	161
实训1 交换机端口安全配置	162
实训2 IP 访问控制列表	171
任务1 标准访问控制列表的	
配置	171
任务2 扩展访问控制列表的	
配置	177
任务3 命名访问控制列表的	
配置	183
实训3 网络地址转换	189
任务1 利用动态 NAPT 实现	
局域网访问 Internet	189
任务2 利用 NAT 实现外网主	
机访问内网服务器	197
项目6 广域网技术实现	204
实训1 路由器的广域网协议配置	205
任务1 路由器的广域网	
HDLC 封装	205



任务 2 路由器的广域网 PPP 封装..... 211	实训 2 无线网络的安全管理 234
实训 2 路由器的广域网 PPP 封装 验证..... 217	实训 3 有线和无线网络的全网 互连..... 239
任务 1 路由器的广域网 PPP 封装 PAP 验证 217	项目8 防火墙技术实现 246
任务 2 路由器的广域网 PPP 封装 CHAP 验证..... 221	实训 1 防火墙的基本配置 247
项目7 无线网络技术实现 226	实训 2 防火墙 DMZ 技术 252
实训 1 无线网络的基本配置..... 227	项目9 综合实训..... 259
	实训 1 小型企业的网络工程 案例.....259
	实训 2 企业网络综合实训 264



Cisco Packet Tracer 6.1 Instructor 模拟器的使用

项目学习说明

网络设备模拟器是指可以利用软件虚拟出相应的网络设备，并利用这些虚拟出来的网络设备进行连接及相关配置，用来验证或解决相应网络问题的虚拟软件。目前，社会上存在很多网络设备模拟器，如 H3C 网络设备模拟器和 Cisco Packet Tracer 6.1 Instructor 模拟器等。一款优秀的网络设备模拟器，功能全面、强大，可用于模拟网络的搭建、配置、运行，是网络管理员和网络技术学习者必不可少的一款工具，而 Cisco Packet Tracer 6.1 Instructor 模拟器恰恰证明了这一点。

本项目重点学习 Cisco Packet Tracer 6.1 Instructor 模拟器的安装和基本使用方法。

学习能力目标

实训 1：安装 Cisco Packet Tracer 6.1 Instructor 模拟器。

实训 2：使用 Cisco Packet Tracer 6.1 Instructor 模拟器搭建网络。

职业能力目标

能正确安装 Cisco Packet Tracer 6.1 Instructor 模拟器并进行汉化。

能正确使用 Cisco Packet Tracer 6.1 Instructor 模拟器搭建网络拓扑。



实训1 安装 Cisco Packet Tracer 6.1 Instructor 模拟器

学习情境

海成公司由于业务规模的扩大，购置了思科公司的路由器，但管理员对思科设备并不熟悉，于是管理员通过互联网找到思科的模拟器来进行学习。

情境分析

管理员可通过 Internet 在 Cisco 的官方网站下载最新版本的 Cisco Packet Tracer 6.1 Instructor 模拟器，也可以使用本书配套资源中提供的安装包文件，掌握 Cisco Packet Tracer 6.1 Instructor 模拟器的安装及汉化操作，是每个学习者必须掌握的。

本实训要求重点掌握 Cisco Packet Tracer 6.1 Instructor 模拟器的安装和汉化操作。

步骤实现

步骤 1：将下载好的 Cisco Packet Tracer 6.1 Instructor 模拟器安装文件及汉化语言包文件进行解压，双击 Cisco Packet Tracer 6.1 for Windows (no tutorials) - Instructor version 文件，进入软件的安装界面，如图 1-1-1 所示。

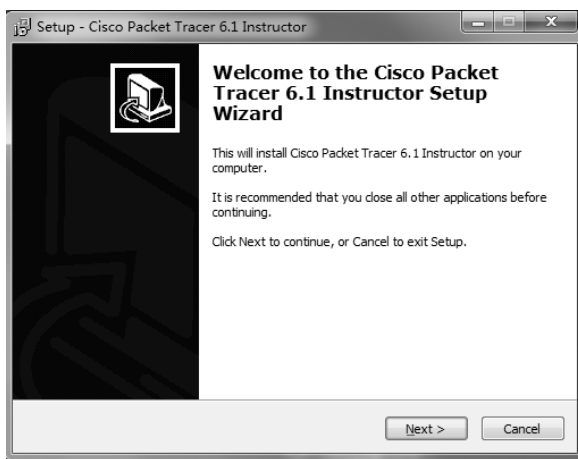


图 1-1-1 Cisco Packet Tracer 6.1 Instructor 的安装界面

步骤 2：单击“Next”按钮，进入安装许可协议界面，如图 1-1-2 所示。

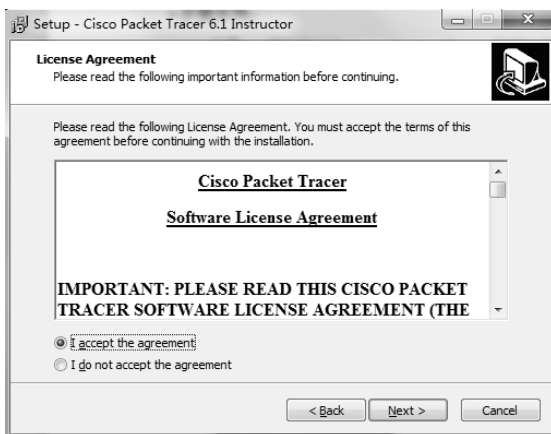


图 1-1-2 Cisco Packet Tracer 6.1 Instructor 安装许可协议界面

步骤 3: 在图 1-1-2 中选中 “I accept the agreement” 单选按钮, 单击 “Next” 按钮, 进入安装路径设置界面, 如图 1-1-3 所示。

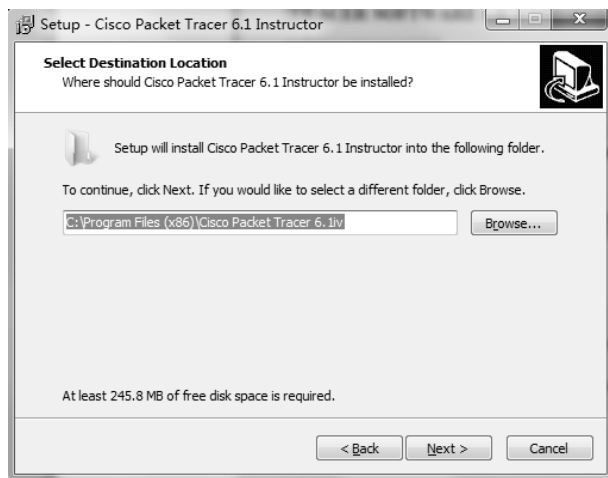


图 1-1-3 Cisco Packet Tracer 6.1 Instructor 安装路径设置界面

步骤 4: 在图 1-1-3 中使用默认安装路径进行安装, 此路径在后面进行汉化操作时需要用到。从图 1-1-3 中可以看到, 安装路径为 “C:\Program Files(x86)\ Cisco Packet Tracer6.1iv”。单击 “Next” 按钮, 进入 “Select Start Menu Folder” 界面, 如图 1-1-4 所示。

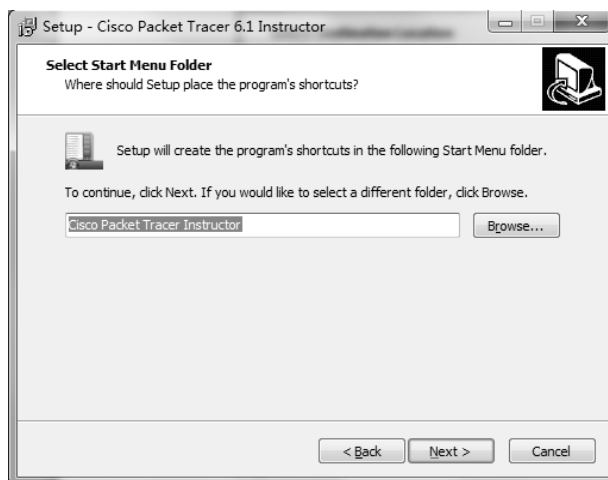


图 1-1-4 “Select Start Menu Folder” 界面

步骤 5: 在图 1-1-4 中使用默认名称作为 “开始” 菜单中的名称, 单击 “Next” 按钮, 进入 “Select Additional Tasks” 界面, 如图 1-1-5 所示。

步骤 6: 在图 1-1-5 中默认选中 “Create a desktop icon (建立桌面图标)” 复选框, 单击 “Next” 按钮, 进入 “Ready to Install” 界面, 如图 1-1-6 所示。

步骤 7: 在图 1-1-6 中单击 “Install” 按钮, 进入软件安装界面, 如图 1-1-7 所示。

步骤 8: 安装完成后会弹出软件安装完成对话框, 先单击 “确定” 按钮, 表示确定使用此版本的软件, 再单击 “Finish” 按钮, 如图 1-1-8 所示。

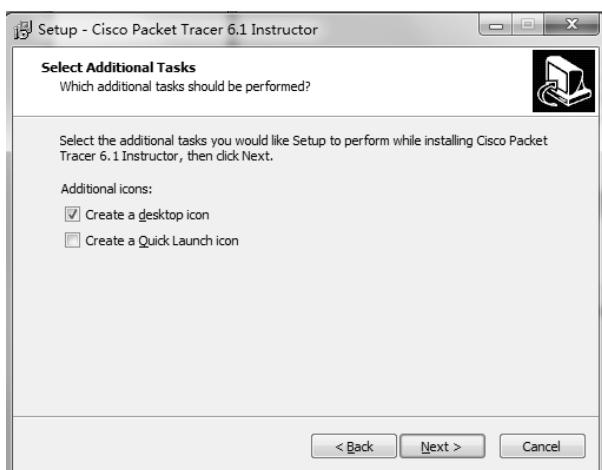


图 1-1-5 “Select Additional Tasks” 界面

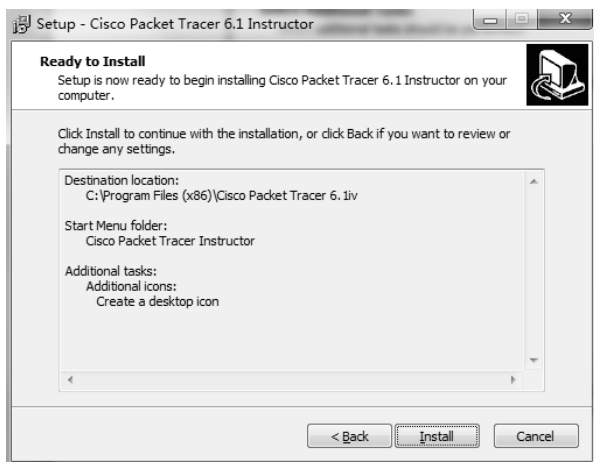


图 1-1-6 “Ready to Install” 界面

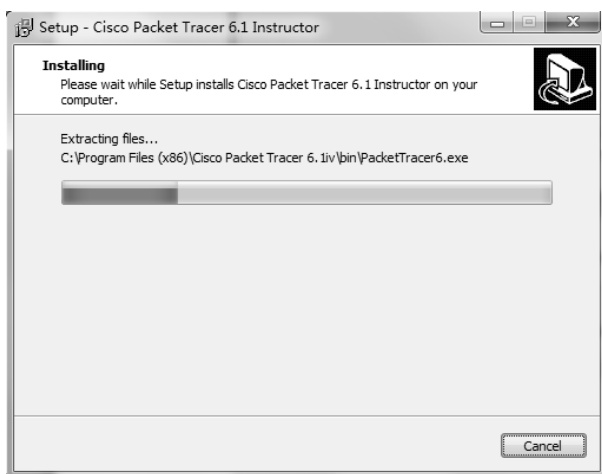


图 1-1-7 Cisco Packet Tracer 6.1 Instructor 软件的安装过程



图 1-1-8 安装完成

步骤 9：系统弹出提示对话框，提示用户保存文件的路径，单击“OK”按钮，如图 1-1-9 所示。

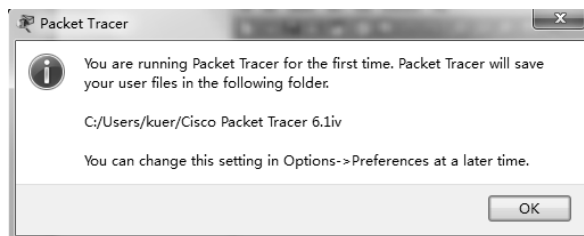


图 1-1-9 用户保存路径

步骤 10：系统会自动打开 Cisco Packet Tracer 6.1 Instructor 软件主窗口，如图 1-1-10 所示。

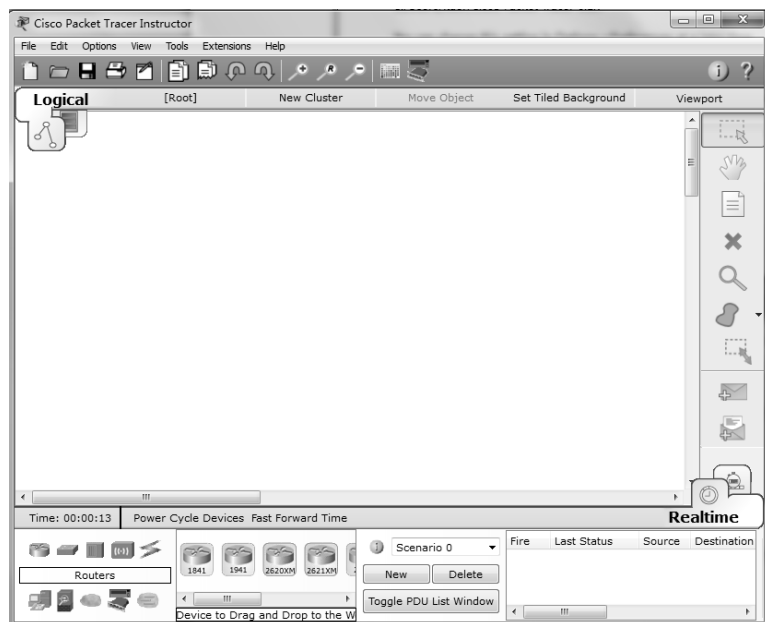


图 1-1-10 Cisco Packet Tracer 6.1 Instructor 软件主窗口



步骤 11: Cisco Packet Tracer 6.1 Instructor 模拟器默认是英文操作界面，为了更好地掌握和学习该软件，还可以进一步对 Cisco Packet Tracer 6.1 Instructor 模拟器进行汉化。在汉化前最好先关闭已经开启的 Cisco Packet Tracer 6.1 Instructor 模拟器。

步骤 12: 复制软件包中的 Chinese.ptl 文件到 Cisco Packet Tracer 6.1 Instructor 模拟器安装目录的“languages”文件夹中，如图 1-1-11 所示。

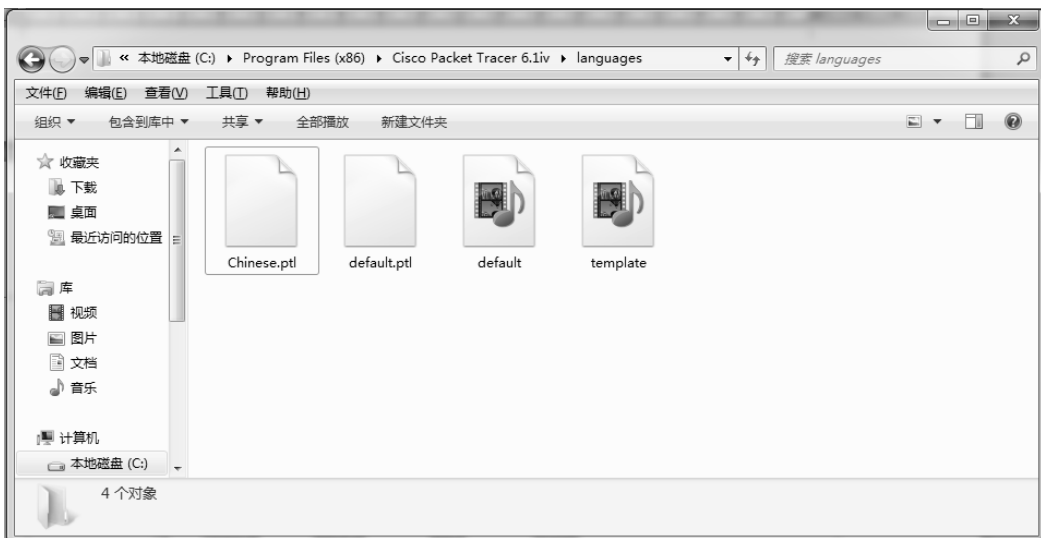


图 1-1-11 复制 Chinese.ptl 文件到安装目录中

步骤 12: 重新启动 Cisco Packet Tracer 6.1 Instructor 模拟器，选择“Option”→并选择“Preference”选项，弹出软件属性配置对话框，如图 1-1-12 所示。

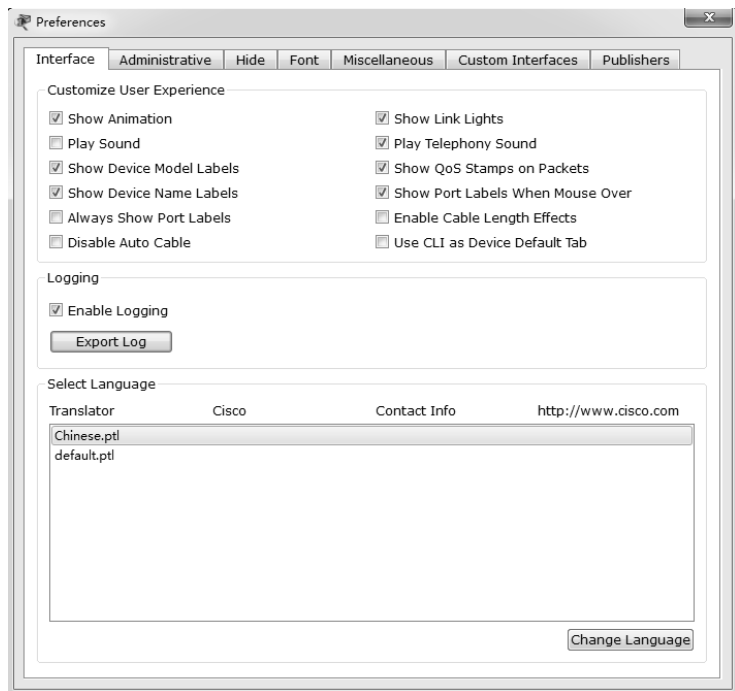


图 1-1-12 Cisco Packet Tracer 6.1 Instructor 模拟器属性配置对话框

步骤 13: 在如图 1-1-12 所示的对话框中可以进行许多设置, 如要使用软件的声效。可以选中“Play Sound”复选框。而实现汉化操作则在“Select Language”选项组中选择“Chinese.ptl”选项, 单击“Change Language”按钮。

步骤 13: 弹出如图 1-1-13 所示的对话框, 提示重新启动软件后新的语言包将会生效。单击“OK”按钮, 完成软件的汉化操作, 如图 1-1-14 所示。

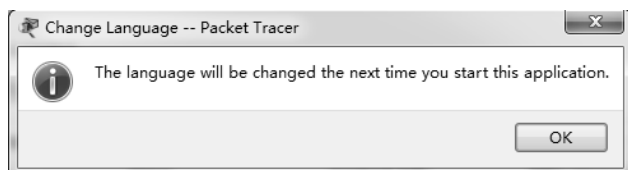


图 1-1-13 提示重新启动软件

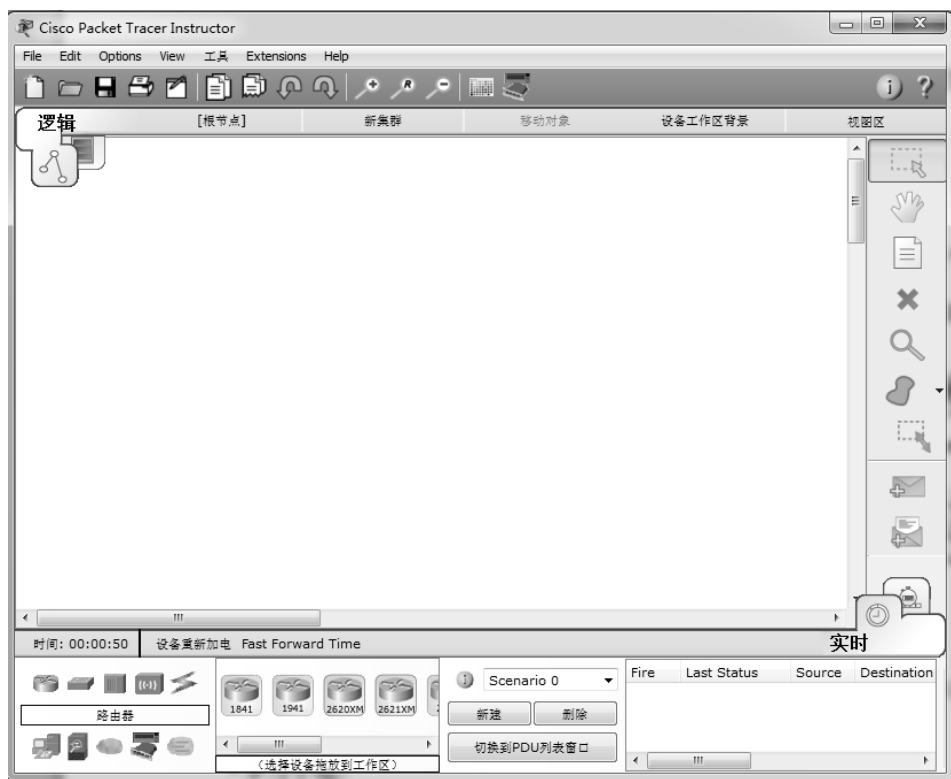


图 1-1-14 Cisco Packet Tracer 6.1 Instructor 汉化成功



小贴士

这里需要注意的是, Cisco Packet Tracer 6.1 Instructor 的汉化操作并非完全的汉化, 部分操作还是以英文来显示的。

相关知识

Cisco Packet Tracer 6.1 Instructor 是一款非常实用的网络设备模拟软件, 其特点是界面直观、操作简单、帮助功能强大、容易上手, 非常适合初学者或在校生网络互联课程的实验教学。要利用 Cisco Packet Tracer 6.1 Instructor 来构建网络互联实验环境, 首先要配置好软件环境。



课堂训练

教师将安装软件包放入学生共享中，使每个学生根据步骤进行安装，并将其汉化，学生操作完成后，教师进行检查和验证。

学习小结

本实训重点讲述了 Cisco Packet Tracer 6.1 Instructor 的安装过程和汉化过程。安装过程和汉化过程比较简单，和其他应用软件安装过程类似。Cisco Packet Tracer 6.1 Instructor 对硬件的要求不高，在学校的各个实验中均可安装使用，因此也可在家庭计算机上安装和使用，增加学生动手操作的机会和熟练程度。Cisco Packet Tracer 6.1 Instructor 是一款免费的共享软件，不需要注册。

实训 2 使用 Cisco Packet Tracer 6.1 Instructor 搭建网络

学习情境

海成公司的管理员安装 Cisco Packet Tracer 6.1 Instructor 软件后，还不太会使用该软件搭建网络，于是准备使用该软件搭建一个网络拓扑，用于以后的学习。

情境分析

如果在 Cisco Packet Tracer 6.1 Instructor 中进行一组网络实验，则首先要搭建好用于实验的网络拓扑结构，这就要求用户掌握如何在 Cisco Packet Tracer 6.1 Instructor 中添加网络设备，以及相邻的网络设备如同进行互连。

本实训重点学习网络设备的添加与连线，实训拓扑如图 1-2-1 所示。

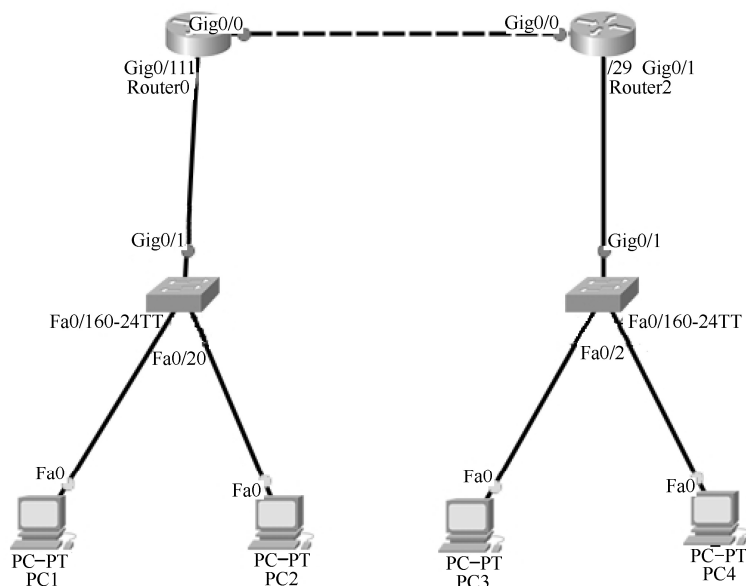


图 1-2-1 基于路由器和交换机的网络拓扑

步骤实现

步骤 1：添加网络设备并更改标签名。在软件主窗口的设备选择区可以看到许多不同种类的网络设备，从左至右、从上到下依次为路由器、交换机、集线器、无线设备、设备

之间的线缆、终端设备、防火墙、仿真广域网，以及自定义设备，如图 1-2-2 所示。

步骤 2：首先在设备选择区内找到要添加的网络设备的大类别，再从该类别的设备型号中寻找自己想要的设备，最后将其拖动到工作区即可完成添加设备的操作。例如，在本实训中添加一个型号为 2911 的路由器，如图 1-2-3 所示。添加完成后在工作区可以看到一个标签名为“Router0”的 2911 路由器的图标。单击该标签，可以进入标签的编辑状态，更改标签名为“Router-A”。



图 1-2-2 设备选择区

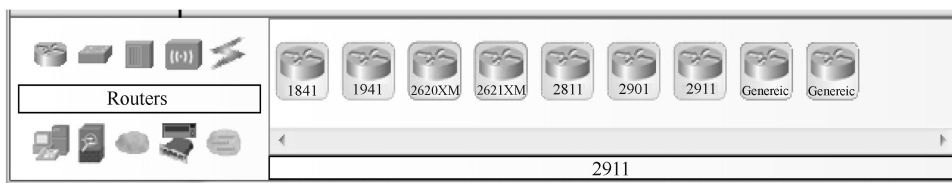


图 1-2-3 添加 2911 路由器

步骤 3：用同样的办法，可以添加其他网络设备和更改标签名，添加完成后可以通过鼠标拖动的方式调整各个设备之间的位置关系，如图 1-2-4 所示。

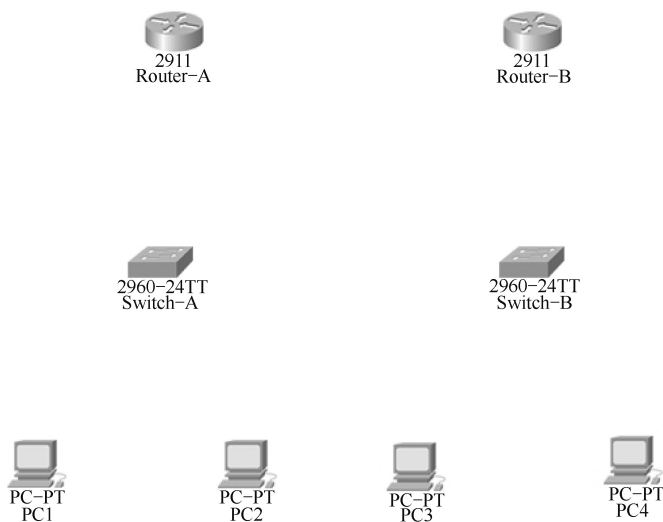


图 1-2-4 添加所需的网络设备

步骤 4：认识网络连接的线缆。当添加好网络设备时，每个设备都是独立的，要进行网络配置实验，还要进行设备的连线。Cisco Packet Tracer 6.1 Instructor 中对设备的连线要求是非常严格的。不同的设备、不同的接口之间需采用不一样的线缆进行连接，否则不能连通。因此，连接设备时要特别注意。

当在设备选择区中选中线缆时，从右侧可以看到有许多不同的线缆类型，如图 1-2-5 所示，依次为自动选择类型、控制线、直通线、交叉线、光纤、电话线、同轴电缆、DCE 串口和 DTE 串口线、Octal 线。



图 1-2-5 Cisco Packet Tracer 6.1 Instructor 中的线缆类型

(1) 自动选择类型：自动连线，可通用，一般不建议使用，除非真的不知道设备之间该使用什么类型的连线。

(2) 控制线：用来连接计算机的 COM 端口和网络设备的 Console 端口。

(3) 直通线：双绞线两端采用同一种线序标准制作的网线，一般用来连接不同网络设备的以太网口，如计算机与交换机、交换机与路由器的以太网口。

(4) 交叉线：双绞线两端采用不同线序标准制作的网线，一般用来连接相同或相似网络设备的以太网口，如计算机与计算机、计算机与路由器、路由器与路由器的以太网口。

(5) 光纤：又称光导纤维，是软而细的、利用内部全反射原理来传导光束的传输介质。用于连接光纤设备，如交换机的光纤模块。

(6) 电话线：用于连接 Modem（调制解调器）或路由器的基本电话连接服务的 RJ-11 端口的模块。

(7) 同轴电缆：现行以太网同轴电缆的接法有两种，一种为直径 0.4cm 的 RG-11 粗缆，采用凿孔接头接法；另一种为直径 0.2cm 的 RG-58 细缆，采用 T 形头接法。

(8) DCE 串口和 DTE 串口线：用于路由器广域网接入。在实际应用当中，需要把 DCE 串口线和一台路由器相连，DCE 串口线和另一台设备相连。但在 Cisco Packet Tracer 6.1 Instructor 中，只需选一根即可。若选择了 DCE 线，则和这条线相连的路由器为 DCE 端，需要配置该路由器的时钟。

(9) Octal 线：俗称“八爪线”，用于连接多台设备。通过 CAB-OCTAL-ASYNC 电缆在一个异步接口上引出 8 条电缆连接到 8 台设备的 Console 端口。

步骤 5：使用线缆连接设备。当网络设备添加好之后，选择相应的线缆，然后在要进行连线的网络设备上单击。在本实训中为 PC1 与 Switch-A 进行连接时使用直通线，单击 PC1 时会进入如图 1-2-6 所示的端口选择界面，选中要进行连接的端口，再移动到 Switch-A 上单击，选中适当的接口即可连接。



图 1-2-6 连接网络设备的端口

步骤 6：使用步骤 5 的方法，可以对其他设备进行连接。完成后的网络拓扑图应该与图 1-2-1 相似。

知识拓展

1. 显示拓扑图中所有设备的端口

完成网络搭建后，可能无法看到设备之间使用的端口，可以通过选择“Option”→“Preference”选项，弹出如图 1-2-7 所示的软件属性配置对话框，选中“Always Show Port Labels”（总显示端口标签）复选框来进行设置。



图 1-2-7 属性配置对话框

2. 设备编辑工具箱的使用

设备编辑工具箱如图 1-2-8 所示。

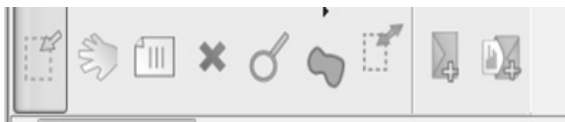


图 1-2-8 设备编辑工具箱

使用设备编辑工具箱可以对设备进行编辑。设备编辑工具箱从左至右依次为选择、更改布局、笔记、删除、查看、增加简单协议数据单元和增加复杂协议数据单元。

- (1) 选择：选中一个设备或线缆，可以移动设备的位置。
- (2) 更改布局：总体移动。当网络拓扑比较大时，可以使用它进行移动查看。
- (3) 笔记：用来添加注释，使用户看得更清楚明白。
- (4) 删除：使用此工具可以删除一个或多个设备、线缆和注释等。
- (5) 查看：选中后，在路由器和 PC 上可以看到各种表，如路由表等。

3. 熟悉鼠标的操作

鼠标操作分为单击、拖动和框选。

- (1) 单击：单击任意一个设备，将打开该设备的配置面板。
- (2) 拖动：拖动任意一个设备，可以重新调整该设备在界面中的位置。
- (3) 框选：可以选中多个设备，结合拖动可以同时移动多个选中的设备，从而调整设备的位置。

课堂训练

教师在黑板上画好拓扑结构图，让每个学生使用模拟器完成，学生操作完成后，教师进行检查和验证。



学习小结

本实训重点讲述了添加网络设备时应注意设备的型号，不同型号的设备功能会有很大的区别。不同的设备之间、不同类型的接口使用的连接线缆会有很大的差别，因此进行网络设备连接时要注意正确选择线缆。连接网络时要根据连接要求正确连接各个网络设备的端口。

项目考核

打开模拟器，完成图 1-2-9 所示的拓扑结构图。

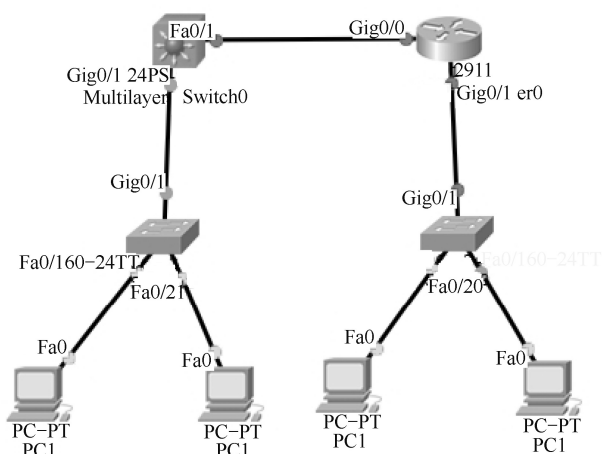
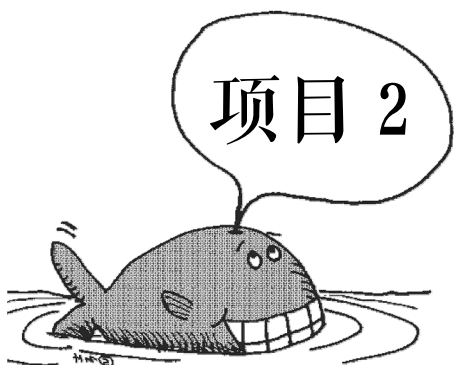


图 1-2-9 拓扑结构图



交换技术基础

项目学习说明

交换技术在现代的高速网络中承担着举足轻重的角色，企业网络依赖交换机分隔网段并实现高速连接。交换机是适应性极强的第二层设备，在简单场景中，可以替代集线器作为多台主机的中心连接点；在复杂应用中，交换机可以连接一台或多台其他交换机，从而建立、管理和维护冗余链路及 VLAN 连通性。对于网络学习者而言，熟悉交换机的配置、熟练掌握交换机的管理是必备的知识 and 技能。

本项目重点学习交换机的基本配置、端口配置、VLAN 划分及管理、生成树协议等内容。

学习能力目标

实训 1：交换机的基本配置。

实训 2：交换机的 VLAN 配置。

实训 3：交换机的常用技术。

职业能力目标

熟悉交换机的各种配置模式。

熟练掌握配置交换机的各项网络参数及接口状态。

学会交换机的配置文件管理。

学会交换机 VLAN 的划分方法。

学会配置交换机间相同 VLAN 通信的方法。

学会配置三层交换机实现不同 VLAN 间通信的方法。



熟练配置交换机链路聚合技术。
理解交换机生成树算法并熟练配置生成树。
学会交换机的 VTP 技术。
会配置 VTP 域中交换机的 VTP 模式及相关参数。
掌握交换机的 DHCP 配置。
学会配置交换机的 HSRP 技术。

实训 1 交换机的基本配置

交换机的基本配置主要有：给设备命名、登录信息、设置特权密码、VTY 密码及 Telnet 管理、端口配置等。本实训分为以下 4 个任务进行学习。

- 任务 1 交换机的几种配置模式。
- 任务 2 交换机的基本配置。
- 任务 3 交换机的备份与升级。
- 任务 4 交换机的 Telnet 配置。

任务 1 交换机的几种配置模式

交换机的配置模式有许多，主要包括用户配置模式、特权模式、全局配置模式、端口配置模式和 VLAN 配置模式等。熟练掌握各种配置模式的进入与切换，了解各种模式下的配置命令，将为以后的学习打下良好的基础。

学习情境

海成公司为组建局域网，新购置了一批 Cisco Catalyst 2960 系列以太网交换机，实现设备的接入。在接入之前需要先熟悉交换机的配置模式及基本配置命令。

情境分析

在工作区添加一台 Cisco Catalyst 2960 交换机，交换机的 Console 端口与 PC 的 COM1 端口互连，使用交换机出厂随机配置的专用控制线连接，此时交换机为出厂配置，使用交换机管理的“命令行”界面进行操作，练习交换机的多种配置模式的切换。



所需设备：

- (1) Cisco Catalyst 2960 交换机 1 台。
- (2) 带超级终端应用程序的 PC 1 台。
- (3) 交换机的 Console 线 1 条。

任务拓扑结构如图 2-1-1 所示。

步骤实现

步骤 1：按照图 2-1-1，连接网络拓扑结构图。

步骤 2：单击 PC 1，在打开的窗口中选择“Desktop”选项卡，进入如图 2-1-1 拓扑结构 图 2-1-2 所示界面，选择“Terminal”（超级终端）选项，将其打开。

步骤 3：弹出“终端配置”对话框，调整超级终端的参数，如图 2-1-3 所示，单击“确定按钮。”



图 2-1-2 PC 桌面应用程序



图 2-1-3 “终端配置”对话框

步骤 4: 进入交换机配置页面，等待交换机装载系统文件，当出现如下提示时，表示系统启动完成。

```
Cisco Internetwork Operating System Software
IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE
SOFTWARE(fcl)
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 18-May-05 22:31 by jharirba

Press RETURN to get started!
```

步骤 5: 此时按回车键即可进入交换机的用户配置模式。此时显示交换机的默认主机名为 Switch，该模式下的提示符为“>”。在该模式下可使用的命令比较少，可以使用“?”命令显示该模式下的所有命令。

```
Switch>?
Exec commands:
connect      Open a terminal connection
```



```
disable      Turn off privileged commands
disconnect   Disconnect an existing network connection
enable       Turn on privileged commands
exit         Exit from the EXEC
logout       Exit from the EXEC
ping         Send echo messages
resume       Resume an active network connection
show         Show running system information
telnet       Open a telnet connection
terminal     Set terminal line parameters
traceroute   Trace route to destination
Switch>
```

步骤 6：在用户配置模式下输入“enable”命令，进入特权模式。特权模式的提示符为“#”，所以也称“#”模式。特权模式下可对交换机的配置文件进行管理，查看交换机的配置信息，进行网络的测试和调试等。输入“？”可以查看特权模式下的所有命令。

```
Switch>enable
Switch#?
Exec commands:
clear        Reset functions
clock        Manage the system clock
configure    Enter configuration mode
connect      Open a terminal connection
copy         Copy from one file to another
debug        Debugging functions (see also 'undebug')
delete       Delete a file
dir          List files on a filesystem
disable      Turn off privileged commands
disconnect   Disconnect an existing network connection
enable       Turn on privileged commands
erase        Erase a filesystem
exit         Exit from the EXEC
logout       Exit from the EXEC
more         Display the contents of a file
no           Disable debugging informations
ping         Send echo messages
reload       Halt and perform a cold restart
resume       Resume an active network connection
setup        Run the SETUP command facility
show         Show running system information
--More--
```

步骤 7：在全局配置模式下可以配置交换机的全局性参数。在特权模式下输入“config terminal”或者“config t”或者“conf t”即可进入全局配置模式。全局配置模式也称“config”模式，在此配置模式下输入的命令会影响整个交换机的运行环境。

```

Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#?
Configure commands:
access-list      Add an access list entry
banner           Define a login banner
boot             Boot Commands
cdp              Global CDP configuration subcommands
clock            Configure time-of-day clock
crypto           Encryption module
do               To run exec commands in config mode
enable           Modify enable password parameters
end              Exit from configure mode
exit             Exit from configure mode
hostname         Set system's network name
interface        Select an interface to configure
ip              Global IP configuration subcommands
line            Configure a terminal line
logging          Modify message logging facilities
mac             MAC configuration
  mac-address-table  Configure the MAC address table
mls             mls global commands
no              Negate a command or set its defaults
port-channelEtherChannel configuration
privilege        Command privilege parameters
--More--

```

步骤 8：端口配置模式下可以对交换机的端口进行参数配置。一般交换机拥有许多端口，还可以添加不同的模块。默认情况下，交换机的所有端口都是以太网接口类型。进入端口配置模式时，要使用“**interface ethernet<端口 ID>**”命令。

```

Switch(config)#interface f0/1
Switch(config-if)#?
cdp              Global CDP configuration subcommands
channel-groupEtherchannel/port bundling configuration
  channel-protocol  Select the channel protocol (LACP, PAgP)
description       Interface specific description
duplex            Configure duplex operation.
Exit             Exit from interface configuration mode
ip              Interface Internet Protocol config commands
mls             mls interface commands
no              Negate a command or set its defaults
shutdown         Shutdown the selected interface
spanning-tree    Spanning Tree Subsystem
speed           Configure speed operation.
storm-control     storm configuration

```




```
switchport      Set switching mode characteristics
tx-ring-limit   Configure PA level transmit ring limit
```

步骤 9：交换机各模式之间的切换可通过“exit”和“end”命令完成。

```
Switch>enable    ! 从普通用户模式进入特权用户模式
Switch#conf t    ! 从特权用户模式进入全局配置模式
Switch(config)#int f0/1    ! 从全局模式进入到接口配置模式
Switch(config-if)#exit    ! 返回上一级模式
Switch(config)#end    ! 直接返回特权模式
Switch#disable   ! 从特权用户模式切换到普通用户模式
Switch>
```



小贴士

屏幕提示出现“—More”字样时，表示当前输出没有结束，可以按 Space 键继续显示下一屏输出的信息，也可以按 Enter 键，显示下一行输出信息。

配置和管理 Cisco LAN 交换机的方法有多种，如 Cisco Network Assistant、Cisco Device Manager、Cisco IOS CLI、Cisco View 管理软件、SNMP 网络管理产品。配置前需注意当前无线网络的使用情况，防止无线网络中断。

上述的某些方法属于带内管理方式，需要采用 IP 地址或 Web 浏览器来连接交换机，这时需要用到 IP 地址。与路由器接口不同，交换机端口不会获得指定的 IP 地址。要使用基于 IP 地址的管理产品或通过 Telnet 会话来管理 Cisco 交换机，需要为交换机配置管理 IP 地址。

相关知识

虽然构建企业网络时会用到路由器和交换机，但大多数企业的网络主要依赖于交换机。交换机每个端口的成本低于路由器，而且能够以线速快速转发帧。

交换机可以根据帧中的目的 MAC 地址，将消息流从一个端口转发到另一个端口。交换机不能在不同的局域网之间路由流量。在 OSI 模型中，交换机执行第 2 层（数据链路层）功能。

1. 2960 系列独立交换机

Catalyst 2960 系列交换机是固定配置的独立设备，不支持模块和闪存卡插槽。由于不能改变固定配置的交换机的物理配置，因此必须根据所需的端口数和端口类型来决定是否使用此类交换机。Cisco Catalyst 2960 系列智能以太网交换机适用于中小型网络。此系列的交换机支持 10/100b/s 快速以太网以及 10/100/1000b/s 千兆以太网 LAN 连接。2960 交换机的前面板如图 2-1-4 所示。



图 2-1-4 Cisco Catalyst 2960 交换机的前面板

该系列交换机使用 Cisco IOS 软件，用户可使用基于 GUI 的 Cisco Network Assistant 或通过 CLI 对其进行配置。

2. 多层交换机

第 2 层交换机基于硬件。此类交换机通过内部电路在接口之间建立物理连接，以线速转发流量。转发时会用到 MAC 地址及 MAC 表中存在的目的 MAC 地址。第 2 层交换机只能在一个网段或子网内转发流量。

第 3 层交换机[也称多层交换机（Multilayer Switching）]在同一台设备中集成了基于硬件的交换和基于硬件的路由。多层交换机同时兼具第 2 层交换机和第 3 层路由器的功能。多层交换机通常会保存（或称“缓存”）会话中第一个数据包的源和目的路由信息。这样，后续数据包就无需执行路由查找，因为它们可直接在内存中找到路由信息。这一缓存功能提升了设备的性能。

学习小结

本任务介绍了交换机的各个配置模式之间的层次关系，每个模式下均有许多不同的命令，可完成不同的配置，使用“exit”命令可返回上一级模式，使用“end”命令可直接返回特权模式。

任务 2 交换机的基本配置

交换机的基本配置是指对新买回来的交换机进行的基本设置，主要包括交换机的设备命名、时间设置、密码设置、IP 地址配置及默认网关、远程管理配置等。

学习情境

海成公司为组建局域网，新购置了一批 Cisco Catalyst 2960 系列以太网交换机，管理员已经熟悉了交换机的配置模式，下一步需要对交换机做基本配置以便进行管理。

情境分析

为保障交换机的管理安全，需要为交换机配置主机名和口令。给交换机分配地址时，必须将地址分配给虚拟局域网（Virtual Local Area Network VLAN）接口。VLAN 允许将多个物理端口以逻辑形式组合在一起。

所需设备：

- (1) Cisco Catalyst 2960 交换机 1 台。
- (2) 带超级终端应用程序的 PC 1 台。
- (3) Console 线 1 条。

任务拓扑结构如图 2-1-5 所示。

步骤实现

步骤 1：按照图 2-1-5 连接网络拓扑结构。

步骤 2：交换机命名，可使用 hostname 命令将交换机的主机名设置为

SWITCH-A。

```
Switch> ! 用户模式
Switch>enable ! 特权模式
Switch#config t ! 全局配置模式
Switch(config)#hostname SWITCH-A ! 配置主机名
SWITCH-A(config)#
```

步骤 3：交换机在网络中工作时需要给设备设置准确的系统时间，才能与其他设备保持一致。设置系统时间应在交换机的特权模式下设置。配置交换机的系统时间为 2014 年 11 月 22 日 10:00:00。



图 2-1-5 拓扑结构



```
SWITCH-A#Clock set ?          !不清楚命令格式或参数要求时，可以输入? 命令查看  
hh:mm:ss Current Time        !系统提示命令的格式及参数要求  
SWITCH-A#Clock set 10:00:00 22 Nov 2014 !配置系统时间为当前时间  
SWITCH-A#
```

步骤 4：配置控制台密码。为交换机配置一个控制台密码，避免 Console 接口被恶意访问。管理员通过 Console 接口进行配置时需要输入此密码验证身份。因为 Console 接口只有一个，所以默认后面以 0 来表示接口 ID，操作代码如下。

```
SWITCH-A>en  
SWITCH-A#conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
SWITCH-A(config)#line console 0          !进入 Console 0 接口线配置模式  
SWITCH-A(config-line)#password 123       !为 Console 接口配置密码“123”  
SWITCH-A(config-line)#login              !允许通过本地登录，如果没有这此命令，则口令不生效  
SWITCH-A(config-line)#
```

步骤 5：配置交换机特权密码。

```
SWITCH-A>en  
SWITCH-A#conf t  
SWITCH-A(config)#enable password 123456 !配置交换机特权密码为“123456”  
SWITCH-A(config)#enable secret 654321   !配置特权密码为“654321”，以密文形式保存
```



小贴士

一旦普通用户进入特权模式，即可查看交换机全局配置，也可直接输入“config t”命令，进入全局配置模式修改交换机的配置。为保障交换机的安全，应该配置特权密码，限制用户进入特权模式。

配置的密码会保存在交换机的运行配置文件中，以明文保存，用户查看配置时可以看到此密码。如果需要更高的安全级别，则可以用“enable secret”命令配置密码，系统会为指定的密码进行加密保存，在配置文件中也无法看到原密码。

步骤 6：加密所有口令。“enable secret”命令只加密特权密码。如果需要对系统所有密码进行加密存储，则可使用全局配置命令“service password-encryption”。

```
SWITCH-A(config)#service password-encryption !加密系统所有口令  
SWITCH-A(config)#
```

步骤 7：配置交换机的 IP 地址和默认网关。交换机接口 IP 地址的设置在 全局配置模式下进行。默认情况下，二层交换机只有一个 Vlan1 接口，要配置交换机的接口 IP 地址，可以直接对 Vlan1 进行 IP 地址设置。

```
SWITCH-A>enable          !进入特权模式  
Password:                !输入上一步骤配置的特权密码 654321  
SWITCH-A#config terminal !进入全局配置模式  
Enter configuration commands, one per line. End with CNTL/Z.  
SWITCH-A(config)#interface vlan 1 !进入 vlan 1 虚拟接口  
SWITCH-A(config-if)#ip address 192.168.1.1 255.255.255.0 !  
配置交换机的 IP 地址为 192.168.1.1  
SWITCH-A(config-if)#no shutdown !打开交换机 vlan 1 接口，IP 地址生效  
SWITCH-A(config-if)#exit        !返回到全局配置模式  
SWITCH-A(config)#ip default-gateway 192.168.1.254
```

!配置交换机的默认网关，以便与不同网段主机通信

```
SWITCH-A(config)#
```

步骤 8：配置交换机端口双工模式和速度。因为 2960 交换机的端口是支持 10Mb/s、100Mb/s、100Mb/s 多种速率的，在与其他设备互连时，可以使用 **duplex** 接口配置命令来指定交换机端口的双工操作模式。可以指定双工和速度为 **auto**，和对端设备进行协商；也可以手动指定交换机端口的双工模式为 **full**（全双工）或 **half**（半双工），速度可以指定 100Mb/s 或 10Mb/s，以避免厂商间的自动协商问题。

```
SWITCH-A>en
Password:
SWITCH-A#conf t
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH-A(config)#in f0/1      !进入接口配置模式
SWITCH-A(config-if)#duplex ?  !双工模式参数查询
auto  Enable AUTO duplex configuration
full  Force full duplex operation  !选择此选项，强制双工模式为全双工
half  Force half-duplex operation  !选择此选项，强制双工模式为半双工
SWITCH-A(config-if)#duplex auto  !配置双工模式为 auto，自动协商模式
SWITCH-A(config-if)#speed ?
    10   Force 10 Mbps operation
    100  Force 100 Mbps operation
auto  Enable AUTO speed configuration
SWITCH-A(config-if)#speed auto  !配置速度为自动
SWITCH-A(config-if)#end
SWITCH-A#
```

步骤 9：验证配置。在特权模式下输入 “**show running-config**” 命令，也可简写为 “**show run**”，即可查看运行配置文件，验证自己的配置是否正确。

```
SWITCH-A#show run
Building configuration...

Current configuration : 1098 bytes
!
version 12.1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
Hostname SWITCH-A !主机名
!
enable secret 5 $1$mErR$SI6kKbhlkuiS3Lv8zc1kp1 !特权模式密码，密文的
enable password 7 0822455D0A16
! 特权模式密码，明文的，已被 service password-encryption 加密
!
!
!
spanning-tree mode pvst
!
```



```

interface FastEthernet0/1
!
... !物理端口部分无配置，略去显示信息
!
interface FastEthernet0/24
!
interface Vlan1
ip address 192.168.1.1 255.255.255.0 !vlan1 接口地址
!
ip default-gateway 192.168.1.254 !交换机默认网关
!
line con 0 !console 接口
password 7 0822455D0A16
!配置的密码生效，已被 service password-encryption 命令加密存储
login
linev ty 0 4
login
line vty 5 15
login
!
!
end

```

步骤 10：保存交换机配置。

以上步骤所做的配置默认保存在交换机的运行配置文件 `running-config` 中，如果交换机关机或掉电则配置失效，可以把运行配置文件内容保存到开机配置文件 `startup-config` 中，以便永久有效。此操作在特权模式下进行，代码如下。

```

SWITCH-A#
SWITCH-A#copy run
SWITCH-A#copy running-config startup-config !复制运行配置文件到开机配置文件中
Destination filename [startup-config]? !按回车键保留默认目标文件名
Building configuration...
[OK]

```



小贴士

如果在设置了 `enable password` 后又设置了 `enable secret password` 命令，则 `enable secret` 命令会覆盖 `enable password` 命令。

保存运行配置文件时，也可以在特权模式下输入 `write` 命令，把运行配置文件写入到开机配置文件中。

相关知识

默认情况下，交换机中预配置了一个 VLAN（名称为 VLAN 1），用于访问管理功能。

所有交换机都支持半双工或全双工模式。

端口处于半双工模式时，在任意指定的时间内，它只能发送或接收数据，两者不能同时进行。端口处于全双工模式时，能够同时发送和接收数据，吞吐量为半双工情况下的 2 倍。

端口及其所连接的设备必须设置为相同的双工模式。如果设置不相同，则会造成双工不

匹配情况,从而产生大量的冲突,降低通信质量。

交换机端口的速度和双工模式可以手动设置,也可以自动协商。自动协商允许交换机自动检测与端口连接的设备的速度和双工模式。许多 Cisco 交换机上都默认启用自动协商。

要使自动协商能够成功,互连的两台设备必须同时支持该功能。如果交换机启用了自动协商,但其所连接的设备不支持该功能,则交换机会使用所连接设备的速度(10、100 或 1000)并进入半双工模式。如果没有启用自动协商的设备设置为全双工,则默认进入半双工模式,这可能会引发问题。

如果所连接的设备不支持自动协商,则可以在交换机上手动配置双工设置,使其与所连接设备的双工设置匹配。即使连接的端口不支持自动协商,速度参数也能够进行自动调整。

交换机端口设置默认为 Auto-duplex(自动双工)和 Auto-speed(自动速度)。如果一台装有 100 Mb/s 网卡的计算机连接到该端口,则端口会自动进入全双工 100 Mb/s 模式。如果是一台集线器连接到该计算机端口,那么端口一般会进入半双工 10 Mb/s 模式。

使用“show interfaces”命令来查看端口的设置,此命令会生成大量的输出。

学习小结

本任务讲述了交换机的命名方法,即在全局模式下使用 hostname 命令完成,特权密码分为明文和密文两种方式,密文方式更加安全,交换机的接口 IP 地址通过配置 VLAN 的 IP 地址进行设置,交换机的端口速度与双工模式默认为自动调整,命令由手工指定会避免协商中引发的问题。

任务 3 交换机的配置文件管理

交换机的配置文件可以导出保存到本地计算机中,也可从本地上传配置文件到交换机中,使管理员避免重复的操作。运行配置文件可以和导入的配置文件合并,方便对交换机的配置文件进行修改。

学习情境

海成公司在组建局域网过程中,使用的一批交换机配置相同或相似,为避免管理员的重复操作,管理员从一台交换机上导出配置文件,直接上传到其他交换机上稍做修改即可。

情境分析

每个交换机的管理密码、接口状态等基本配置一般相似,但是每台交换机的主机名、管理地址都不相同,可以从一台交换机上完成配置后,导出到本地计算机中,恢复配置到其他交换机中,与其他交换机的运行配置合并生效。

所需设备:

- (1) Cisco Catalyst 2960 交换机 2 台。
- (2) 带超级终端应用程序的 PC 1 台
- (3) 交换机的 Console 线 1 条。
- (4) 直通线 1 条。

任务拓扑结构如图 2-1-6 所示。

步骤实现

步骤 1: 按照图 2-1-6 连接网络拓扑结构。

步骤 2: 配置交换机 1 的主机名为 SWITCH-A,管理地址为 192.168.10.1,默认网关为 192.168.10.254,控制台密码和特权密码分别为 cisco 和 class。

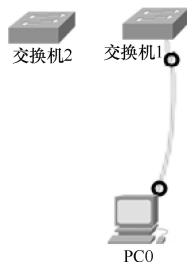


图 2-1-6 拓扑结构



```
SWITCH-A>enable
SWITCH-A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWITCH-A(config)#in vlan 1
SWITCH-A(config-if)#ip add 192.168.10.1 255.255.255.0
SWITCH-A(config-if)#no shutdown

SWITCH-A(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up

SWITCH-A(config-if)#exit
SWITCH-A(config)#line con 0
SWITCH-A(config-line)#pass cisco
SWITCH-A(config-line)#login
SWITCH-A(config-line)#exit
SWITCH-A(config)#enable secret class
SWITCH-A(config)#exit
SWITCH-A#
```

步骤 3：对 SWITCH-A 交换机的配置进行验证。

```
SWITCH-A#sh run
Building configuration...

Current configuration : 1126 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
Hostname SWITCH-A
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCil
!
!
spanning-tree mode pvst
!
interface FastEthernet0/1
...!接口部分无配置，略去显示信息
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.10.1 255.255.255.0
!
```

```

line con 0
password cisco
login
!
end

```

步骤 4: 单击交换机, 在打开的窗口中选择“Config”选项卡, 如图 2-1-7 所示。

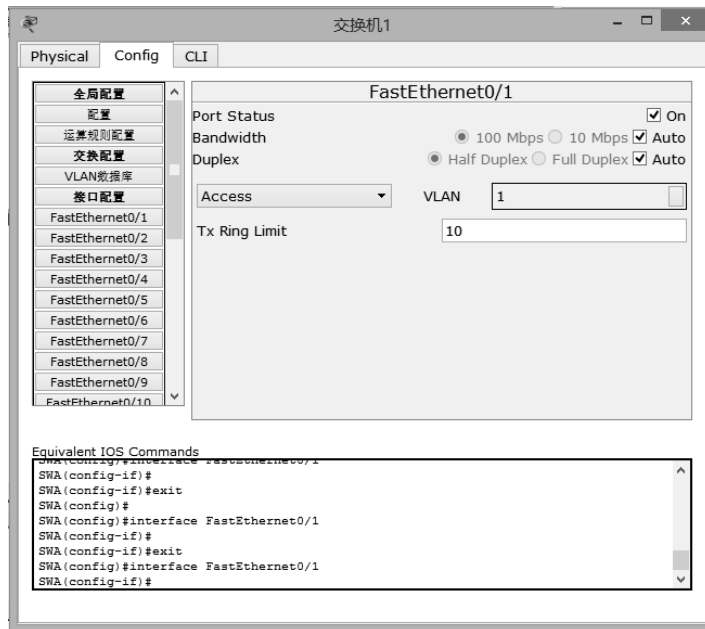


图 2-1-7 “Config”选项卡

步骤 5: 选择“全局配置”选项, 右侧显示全局配置, 如 2-1-8 所示。



图 2-1-8 全局配置



步骤 6：单击运行内存右侧的“保存”按钮，即把当前运行配置文件保存到开机配置文件中，如果单击“消除”按钮，则删除开机配置文件。

步骤 7：导出配置文件到本地。单击“启动配置”右侧的“导出”按钮，随即弹出保存文件对话框，指定文件名和保存位置，后单击“保存”按钮即可，如图 2-1-9 所示。

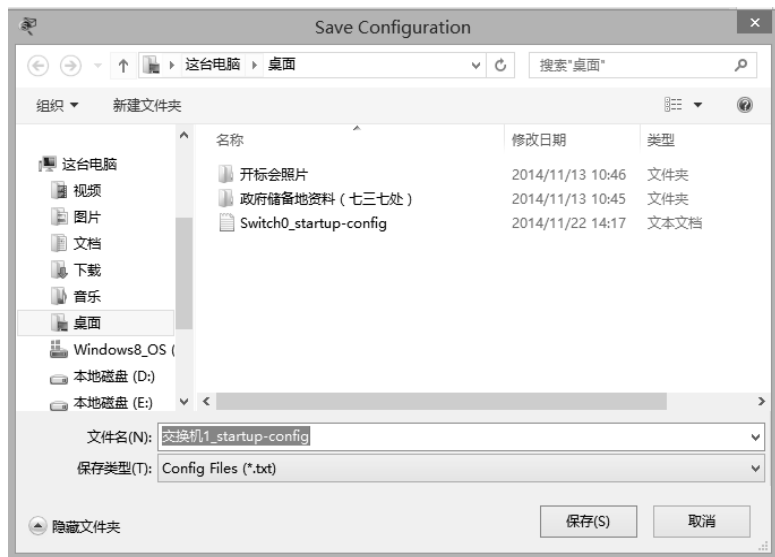


图 2-1-9 保存配置文件

步骤 8：查看配置文件。在资源管理器中找到刚下载的文件，用记事本程序打开，可以查看配置文件的内容，如图 2-1-10 所示。



图 2-1-10 查看本地配置文件

步骤 9：进入管理配置文件。单击交换机 2，在打开的窗口中选择“Config”选项卡，选择“全局配置”选项，进入如图 2-1-11 所示界面。

步骤 10：选择要上传的配置文件。单击“运行配置”右侧的“载入”按钮，在弹出的“Load Configuration”对话框中选择要上传的配置文件，单击“打开”按钮，如图 2-1-12 所示。

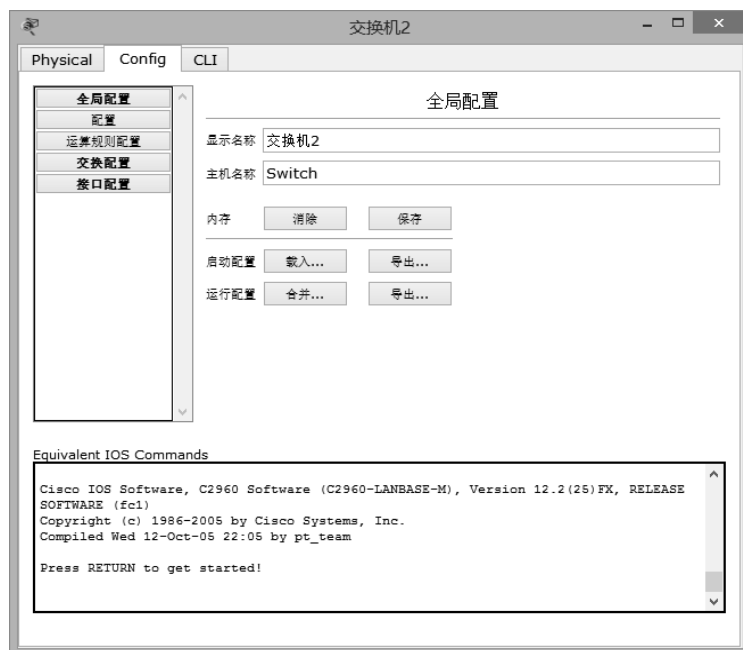


图 2-1-11 交换机 2 的配置文件管理页面

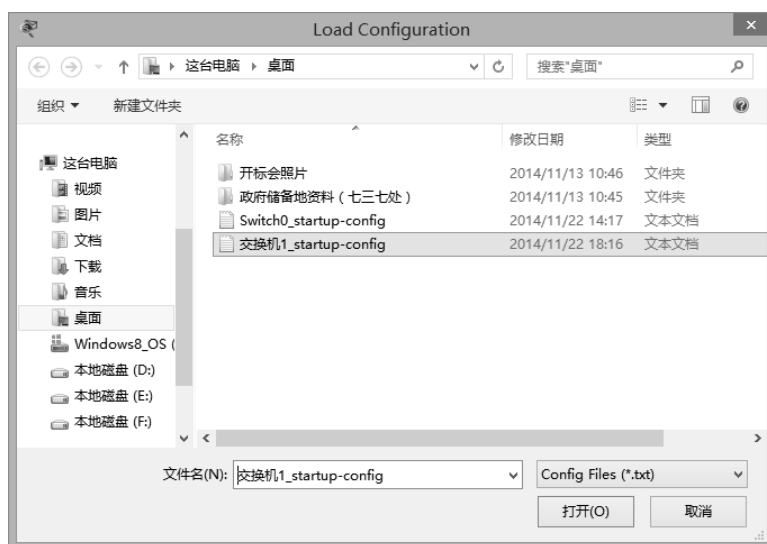


图 2-1-12 导入配置文件对话框

步骤 11: 上传成功后系统会弹出如图 2-1-13 所示的提示对话框。此时系统的运行配置已经改变与 SWITCH-A 相同, 根据需要修改交换机 2 的主机名和管理地址即可。



图 2-1-13 加载配置文件成功



小贴士

在运行配置中导入配置文件后会覆盖当前的运行配置文件，需要修改的配置最好在导入后再操作。

在启动配置中导入配置文件也可以加载配置文件到交换机中，但是需要在特权模式下使用 reload 命令重启交换机才能生效。

相关知识

网络技术人员经常执行的工作是加载交换机配置。运行配置保存在 DRAM 中，而启动配置存储在闪存的 NVRAM 部分中。当使用 copy running-config startup-config 命令时，Cisco IOS 将把运行配置复制到 NVRAM 中，这样，当交换机启动时，它将加载含有新配置的 startup-config。

如果想在设备上保留多个不同的 startup-config 文件，则可以使用“copy startup-configflash: filename”命令将配置复制到不同文件名的多个文件中。存储多个 startup-config 版本可在配置出现问题时回滚到某个时间点。例如，以下操作可在系统 Flash 中存储一个备份配置文件，在某个时间点，可以恢复 Flash 中的备份配置为当前配置文件。

```
SWITCH-A#copy system:running-configflash:startup-config
Destination filename [startup-config]?
SWITCH-A#copy startup-config flash:config.bak1
Destination filename [config.bak1]?
SWITCH-A#copy flash:config.bak1 startup-config
Destination filename [startup-config]?
SWITCH-A#reload
```

使用 reload 命令后，系统将提示是否要保存配置。通常情况下回答“yes”，但是本例中需要回复“no”。如果回复“yes”，则刚刚恢复的文件将被覆盖。任何情况下，都需要考虑当前运行配置是否要在交换机重新加载后成为生效的配置。

学习小结

本任务讲述了怎样将交换机的运行配置文件保存在内存中，如果不保存到启动配置中，则重新开机后会配置就会丢失。交换机的启动配置文件可以下载到本地保存，也可以直接从本地上传启动配置文件。

任务4 交换机系统的备份与升级

网络设备的操作系统文件（Cisco 的操作系统是 IOS、H3C 的是 VRP）是可以导出的，以便对其进行备份。当由于网络操作失误而使网络设备操作系统崩溃时，可将备份的网络操作系统还原出来。

学习情境

海成公司由于业务的扩大，想在网络中增加新的功能，但发现其中的一台交换机版本较低，管理员想对这台交换机进行 IOS 的升级。

情境分析

要对交换机进行 IOS 的升级，首先要在版本高的交换机上备份 IOS，所以管理员要先从其他交换机上备份 IOS，再对版本较低的交换机进行升级。

所需设备：

- (1) Cisco Catalyst 2960 交换机 2 台。

- (2) 带超级终端应用程序的 PC 1 台。
 - (3) 安装好 TFTP 软件的 PC 1 台。
 - (4) Console 线 1 条。
- 任务拓扑结构如图 2-1-14 所示。

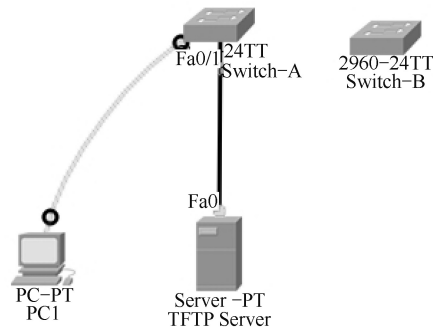


图 2-1-14 拓扑结构

网络参数的设置如表 2-1-1 所示。

表 2-1-1 网络参数设置

设 备	端 口	IP 地址	子网掩码
Switch-A	Vlan1	192.168.1.100	255.255.255.0
TFTP Server		192.168.1.10	255.255.255.0

步骤实现

- 步骤 1：按照图 2-1-14，连接网络拓扑结构图。
- 步骤 2：按照表 2-1-1，配置 TFTP Server 的 IP 地址、子网掩码。
- 步骤 3：配置交换机的主机名称和管理地址。

```
Switch>enable
Switch#config t
Switch(config)#hostname Switch-A
Switch-A(config)#in vlan 1
Switch-A(config-if)#ip add 192.168.1.100 255.255.255.0
Switch-A(config-if)#exit
```

步骤 4：查看交换机的 IOS。

```
Switch-A#show flash:
Directory of flash:/

1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin    !交换机的 IOS

64016384 bytes total (59601463 bytes free)
Switch-A#
```

步骤 5：备份交换机的 IOS。

```
Switch-A#copy flash: tftp:
Source filename []?c2960-lanbase-mz.122-25.FX.bin          !IOS 名称
Address or name of remote host []? 192.168.1.10           !TFTP Server 的 IP 地址
```



```
Destination filename [c2960-lanbase-mz.122-25.FX.bin]?

Writing c2960-lanbase-mz.122-25.FX.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4414921 bytes]

4414921 bytes copied in 3.072 secs (39047 bytes/sec)
Switch-A#
```

步骤 6：在 TFTP Server 中查看备份好的交换机的 IOS，如图 2-1-15 所示。

步骤 7：将 TFTP Server 连接到版本较低的交换机上，如图 2-1-16 所示。

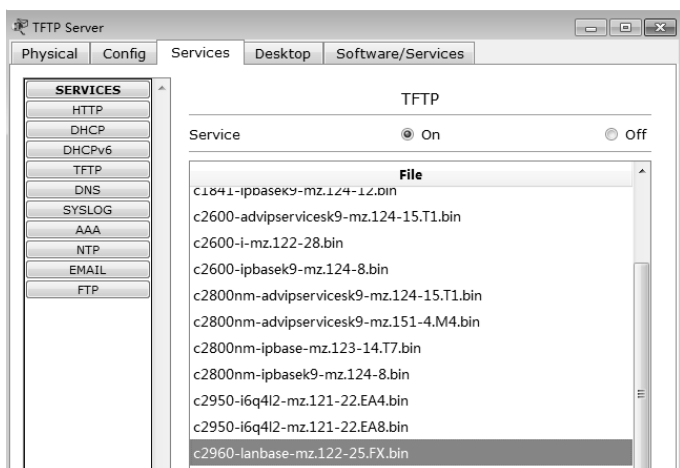


图 2-1-15 查看 TFTP Server 中的 IOS

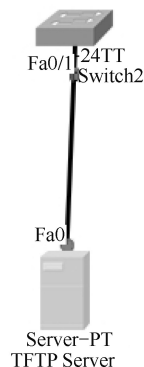


图 2-1-16 连接低版本的交换机网络拓扑

步骤 8：配置交换机 B 的主机名称和管理地址。

```
Switch>enable
Switch#config t
Switch(config)#hostname Switch-B
Switch-B(config)#in vlan 1
Switch-B(config-if)#ip add 192.168.1.200 255.255.255.0
Switch-B(config-if)#exit
```

步骤 9：升级交换机的 IOS。

```
Switch-B#copy tftp: flash:
Address or name of remote host []? 192.168.1.10
Source filename []?c2960-lanbase-mz.122-25.FX.bin
Destination filename [c2960-lanbase-mz.122-25.FX.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]

Accessing tftp://192.168.1.10/c2960-lanbase-mz.122-25.FX.bin...
Loading c2960-lanbase-mz.122-25.FX.bin from 192.168.1.10: !!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 4414921 bytes]
```

```
4414921 bytes copied in 3.067 secs (39111 bytes/sec)
```

```
Switch-B#
```

步骤 10: 查看升级后的 IOS。

```
Switch-B#show flash:
```

```
Directory of flash:/
```

```
1 -rw- 4414921 <no date> c2960-lanbase-mz.122-25.FX.bin
```

```
64016384 bytes total (59601463 bytes free)
```

```
Switch-B#
```

相关知识

交换机的系统文件存储在 Flash 中, 如果 Flash 中的配置文件遭到破坏, 交换机就无法正常工作, 可以通过 TFTP 软件进行恢复, 即从备份的交换机 Flash 文件或互联网下载相关版本的系统文件并写到交换机中。如果系统文件没有损坏, 而交换机的文件丢失了, 则直接恢复文件即可。

TFTP (Trivial File Transfer Protocol, 简单文件传输协议) 是 TCP/IP 协议簇中的一个用来在客户机与服务器之间进行简单文件传输的协议, 提供不复杂、开销不大的文件传输服务。其端口号为 69。

学习小结

本任务讲述了交换机系统的备份与升级, 在实际工作中, 由于公司的业务规模扩大, 经常需要对网络设备进行升级, 这是管理员必须具备的素质, 所以掌握好备份与升级是非常重要的, 要注意 TFTP 软件的使用方法。

任务 5 交换机的 Telnet 配置

交换机配置了管理地址以后, 在网络连通的情况下, 可以使用 Telnet 进行带内管理。这样管理员可以在远程管理交换机, 使网络设备管理更方便。

学习情境

海成公司在组建局域网时所购置的交换机已经完成了基本配置, 现在全部接入网络, 投入使用。为方便对交换机进行维护, 现在需要配置其 TELNET 功能, 以方便远程管理。

情境分析

Telnet 是 Cisco 交换机上支持 VTY 的默认协议。如果为 Cisco 交换机分配了管理 IP 地址, 则可以使用 Telnet 客户端连接到交换机。但是 VTY 线路并不安全, 可以为 VTY 线路配置密码身份验证来保护通过 VTY 线路对交换机的访问。这可以提高 Telnet 服务的安全性。

所需设备:

- (1) Cisco Catalyst 2960 交换机 1 台。
- (2) 带超级终端应用程序的 PC 1 台。
- (3) Console 线 1 条。
- (4) 直通线 1 条。

任务拓扑结构如图 2-1-17 所示。

网络参数的设置如表 2-1-2 所示。

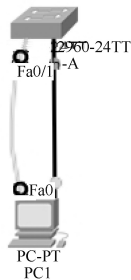


图 2-1-17 拓扑结构



表 2-1-2 网络参数设置

设 备	端 口	IP	子网掩码
Switch-A	Vlan1	192.168.1.100	255.255.255.0
PC1		192.168.1.10	255.255.255.0

步骤实现

步骤 1：按照图 2-1-17 连接网络拓扑结构。

步骤 2：按照表 2-1-2 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置交换机的主机名称和管理地址。

```
Switch>enable
Switch#config t
Switch(config)#hostname Switch-A
Switch-A(config)#in vlan 1
Switch-A(config-if)#ip add 192.168.1.1 255.255.255.0
Switch-A(config-if)#exit
```

步骤 4：配置 Telnet 登录密码。默认情况下，交换机已经开启了 Telnet 管理方式，但不允许远程登录，因此还要做如下配置。

```
Switch-A#
Switch-A#conf t
Switch-A(config)#line vty 0 4                !进入交换机 Telnet 配置模式
Switch-A(config-line)#password abcd          !设置 Telnet 访问密码为“abcd”
Switch-A(config-line)#login                  !允许 Telnet 方式登录
Switch-A(config-line)#exit
Switch-A(config)#
```

步骤 5：保存交换机运行配置。特权模式下使用“copy run start”命令或者“write”命令写入启动配置。

```
Switch-A#write
Switch-A#
```

步骤 6：设置 PC 的 IP 地址。打开 PC 的管理窗口，在“Desktop”选项卡中选择“IP 地址配置”选项，选中“Static”单选按钮，设置 PC 的 IP 地址为 192.168.1.10，子网掩码为 255.255.255.0，如图 2-1-18 所示。

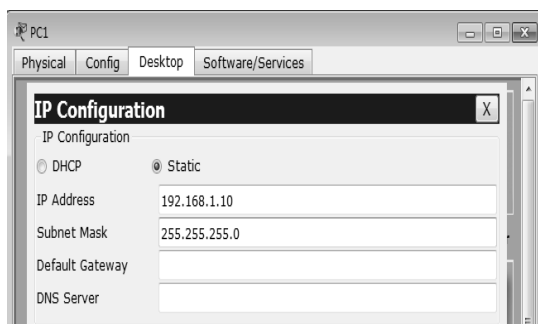


图 2-1-18 PC 的 IP 地址设置

步骤 7：测试 PC 与交换机间的连通性。打开计算机的命令提示符窗口，输入“ping

192.168.1.1”命令，如图 2-1-19 所示，表示 PC 与交换机网络层可以连通。

```
PC>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255
Reply from 192.168.1.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
|
PC>
```

图 2-1-19 测试 PC 与交换机的连通性

步骤 8：尝试从 PC-Telnet 交换机。如果 PC 与交换机网络层可以连通，则可以输入“telnet 192.168.1.1”命令尝试与交换机 Telnet，如图 2-1-20 所示。

步骤 9：进行 Telnet 身份验证。图 2-1-20 中显示了“Open”字样，表示 Telnet 成功，要求输入 Telnet 密码。输入在交换机上配置的 VTY 密码，则可进入交换机的普通用户模式，继续输入特权密码，进入特权模式，与在交换机本地管理配置一样，可以进行交换机管理，如图 2-1-21 所示。

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
```

图 2-1-20 从 PC 尝试与交换机 Telnet

```
PC>
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Password:
SWA>en
Password:
SWA#
```

图 2-1-21 Telnet 身份验证过程



小贴士

此任务中 PC 与交换机直连，所以不需要配置默认网关。在实际应用中，管理员经常跨越三层设备远程管理交换机，所以 PC 必须配置默认网关，二层交换机也相当于一台 PC，需要定义出入本地网络的边界设备——网关。

相关知识

远程访问 Cisco 交换机上的 VTY 接口有两种选择：Telnet 与 SSH。老式交换机可能不支持使用 SSH 的安全通信。

Telnet 是早期型号的 Cisco 交换机上支持使用 SSH 的安全通信的最初方法。Telnet 是用于终端访问的常用协议，因为大部分最新的操作系统都附带内置的 Telnet 客户端。但是 Telnet 不是访问网络设备的安全方法，因为它在网络上以明文形式发送所有通信。攻击者使用网络监视软件可以读取 Telnet 客户端和 Cisco 交换机的 Telnet 服务器之间发送的每一个字符。由于 Telnet 协议存在安全性问题，因此 SSH 成为用于远程访问 Cisco 设备虚拟终端线路的首选协议。



SSH 提供与 Telnet 相同类型的访问，但是增加了安全性。SSH 客户端和 SSH 服务器之间的通信是加密的。SSH 已经有多个版本，Cisco 设备目前支持 SSHv1 和 SSHv2。建议尽可能实施 SSHv2，因为它使用了比 SSHv1 更强的安全加密算法。

知识拓展

SSH 功能有 SSH 服务器和 SSH 集成客户端，后者是在交换机上运行的应用程序。可以使用 PC 上运行的任意 SSH 客户端或交换机上运行的 Cisco SSH 客户端来连接运行 SSH 服务器的交换机。

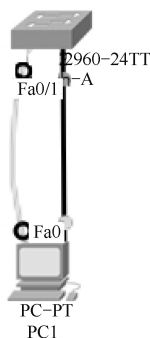


图 2-1-22 拓扑结构

对于服务器组件，交换机支持 SSHv1 或 SSHv2。对于客户端组件，交换机只支持 SSHv1。

所需设备：

- (1) Cisco Catalyst 2960 交换机 1 台。
- (2) 带超级终端应用程序的 PC 1 台。
- (3) Console 线 1 条。
- (4) 直通线 1 条。

实验拓扑结构如图 2-1-22 所示。

网络参数设置如表 2-1-3 所示。

表 2-1-3 网络参数设置

设 备	端 口	IP 地址	子网掩码
Switch-A	Vlan1	192.168.1.1	255.255.255.0
PC1		192.168.1.10	255.255.255.0

步骤实现

步骤 1：按照图 2-1-22 连接网络拓扑结构。

步骤 2：按照表 2-1-3 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置交换机的主机名和域名。

```
Switch>en
Switch#conf t
Switch(config)#hostname Switch-A
Switch-A(config)#ip domain-name abc.com !配置当前交换机所在的域名为 abc.com
Switch-A(config)#
```

步骤 4：设置特权模式密码。

```
Switch-A#
Switch-A#conf t
Switch-A(config)#enable secret 123456 ! 设定特权模式密码
Switch-A(config)#
```

步骤 5：配置 SSH 服务器。

```
Switch-A(config)#username zwk password cisco
! 定义 Telnet 用户名为 zwk，密码为 cisco
Switch-A(config)#line vty 0 15 ! 设定终端连接数为 16
Switch-A(config-line)#login local ! 设定要求登录
```

```
Switch-A(config-line)#exit
```

步骤 6：生成 RSA 密钥。在交换机上启用 SSH 服务器以进行本地和远程身份验证，然后使用“crypto key generate rsa”命令生成 RSA 密钥对。

```
Switch-A(config)#crypto key generate rsa
The name for the keys will be: SA.abc.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```



小贴士

生成 RSA 密钥时，系统提示用户输入模数长度。Cisco 建议使用 1024 位的模数长度。模数长度越长越安全，但是生成和使用模数的时间也会越长。

步骤 7：配置 SSH 服务器的版本。全局模式下使用 ipssh version [1 | 2] 命令将交换机配置为运行 SSHv1 或 SSHv2。

```
Switch-A(config)#ipsshver 2
Switch-A(config)#
```

步骤 8：限制非 SSH 连接。如果要阻止非 SSH 连接，则应在线路配置模式下添加“transport input ssh”命令，将交换机限制为仅允许 SSH 连接。直接（非 SSH）Telnet 连接将被拒绝。

```
Switch-A(config)#line vty 0 15
Switch-A(config-line)#transport input ssh !限制只允许 SSH 登录
Switch-A(config-line)#end
Switch-A#
```

步骤 9：保存设置。

```
Router-A#write                                ! 保存配置
Saving current configuration...
OK!
```

步骤 10：SSH 测试。

(1) 单击 PC1，在打开的 PC1 窗口中选择“Desktop”→“Command Prompt”选项，弹出“Command Prompt”对话框，如图 2-1-23 所示。



图 2-1-23 “Command Prompt”对话框



(2) 在图 2-1-23 所示的对话框中输入“SSH -l zwk 192.168.1.1”命令后按回车键，如图 2-1-24 所示。

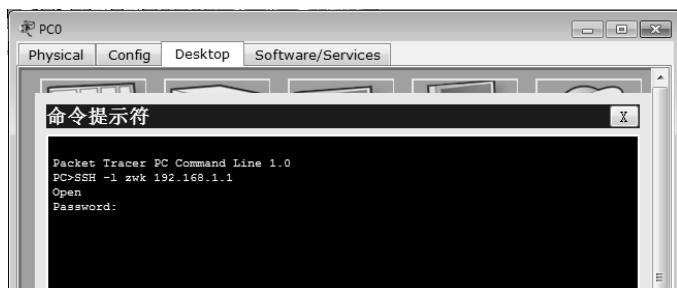


图 2-1-24 连接远程 SSH 路由器

(3) 在“Password”后输入“cisco”，如图 2-1-25 所示，显示“Switch-A>”表示远程登录成功，输入特权密码，即可进入特权模式。

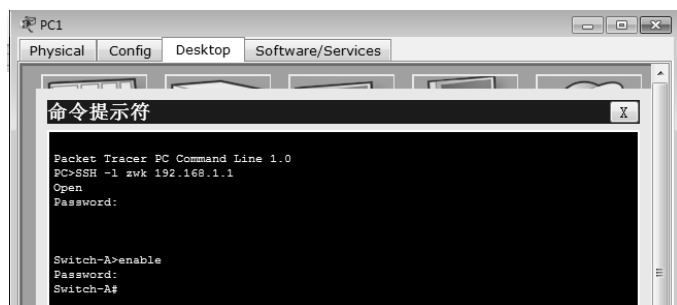


图 2-1-25 SSH 路由器效果图

学习小结

本任务讲述了交换机的 Telnet 和 SSH 的基本配置，需要注意的是，交换机进行 Telnet 连接的前提条件是需要配置 IP 地址使网络连通，访问交换机 VTY 接口有两种选择：Telnet 和 SSH，但 Telnet 属于明文传送的信息，不够安全，而 SSH 使用密钥加密后传送，是推荐使用的带内管理方式。

实训 2 交换机的 VLAN 配置

VLAN 技术在局域网互连时得到了广泛推广和应用。VLAN 是指一个在物理网络上根据用途、工作组、应用等来逻辑划分的局域网络，是一个广播域，与用户的物理位置没有关系。VLAN 中的网络用户是通过 LAN 交换机来通信的。一个 VLAN 中的成员看不到另一个 VLAN 中的成员。

因此，划分 VLAN 能有效地控制网络广播风暴，提高网络的安全可靠性，是有效的网络监控、数据流量控制的手段，还能实现不同地理位置的部门间的局域网通信，有效地节省构建网络时所需网络设备的费用。

本实训将分成以下 3 个任务进行。

任务 1 交换机的 VLAN 划分。

任务 2 交换机间相同 VLAN 的通信。

任务 3 三层交换机的配置。

任务 1 交换机的 VLAN 划分

逻辑上把网络资源和网络用户按照一定的原则划分，把一个物理上的网络分成多个小的逻辑网络，这些逻辑网络就是 VLAN。在接入层交换机上划分 VLAN，可以使一台交换机划分多个 VLAN，从而保证各部门间的安全通信。

学习情境

海成公司的局域网搭建已经完成，为了提高网络的性能和服务质量，现在需要财务部和工程部使用不同的网段，使其相互隔离。

情境分析

为了保证两个部门的相对独立，需要划分对应的 VLAN，使交换机某些端口属于财务部，某些端口属于工程部，这样就能保证它们之间的数据互不干扰，也不影响各自的通信效率。

所需设备：

(1) Cisco Catalyst 2960 交换机 1 台。

(2) PC 4 台。

(3) Console 线 1 条。

(4) 直通线 4 条。

任务拓扑结构如图 2-2-1 所示。

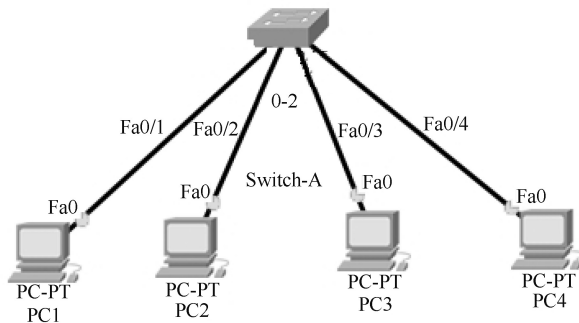


图 2-2-1 交换机的 VLAN 配置

交换机 VLAN 划分及其参数设置，如表 2-2-1 所示。

表 2-2-1 交换机 VLAN 划分及其参数设置

设 备	端 口 成 员	IP 地 址	子 网 掩 码	部 门
Switch 的 VLAN 10	1、2			财务部
Switch 的 VLAN 20	3、4			工程部
PC1	Fa0/1	192.168.1.11	255.255.255.0	财务部
PC2	Fa0/2	192.168.1.12	255.255.255.0	财务部
PC3	Fa0/3	192.168.1.13	255.255.255.0	工程部
PC4	Fa0/4	192.168.1.14	255.255.255.0	工程部



小贴士

二层交换机同一 VLAN 中的端口能够互相通信，不同 VLAN 中的端口不能互相通信。二层交换机不具备路由功能。

而在三层交换机中不同 VLAN 中的端口能够互相通信，因为三层交换机具备路由功能。

步骤实现

步骤 1：按照图 2-2-1 连接网络拓扑结构。

步骤 2：按照表 2-2-1 配置计算机的 IP 地址和子网掩码。

步骤 3：由于分配给每一台计算机的 IP 地址都是 192.168.1.0/24 网段的 IP 地址，所以所有计算机都是相互连通的，如图 2-2-2 所示。

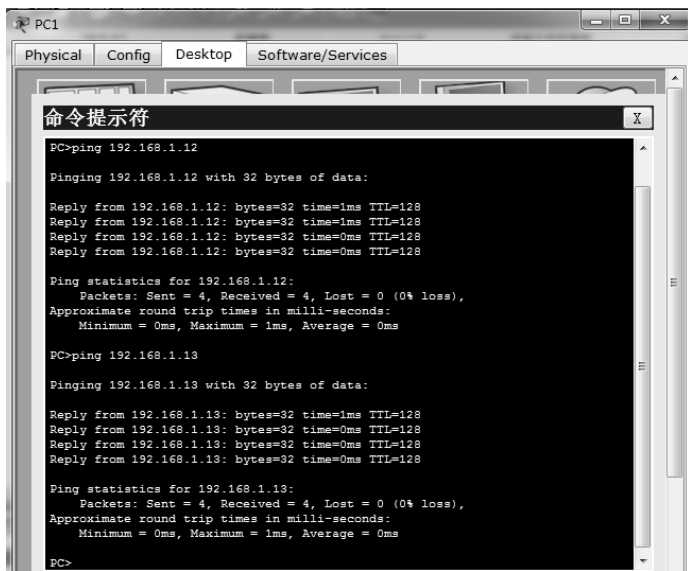


图 2-2-2 划分 VLAN 前测试 PC1 与 PC4 的连通性

步骤 4：在交换机上创建 VLAN 10 和 VLAN 20，并将端口 fa0/1-2 放入 VLAN10，将端口 fa0/3-4 放入 VLAN 20。

```
Switch>en
Switch#conf t
Switch(config)#vlan 10!创建 vlan 10
Switch(config-vlan)#name caiwubu !将 vlan 10 命名为 caiwubu
Switch(config-vlan)#exit !返回全局模式
Switch(config)#vlan 20 !创建 vlan 20
Switch(config-vlan)#name gongchengbu !将 vlan20 命名为 gongchengbu
Switch(config-vlan)#exit !返回全局模式
Switch(config)#in f0/1 !进入接口 f0/1
Switch(config-if)#switchport mode access
!将接口模式改为接入模式，因为是默认接入模式，所以此条命令也可省略
Switch(config-if)#switchport access vlan 10 !把接口加入 vlan 10
Switch(config-if)#in f0/2 !进入接口 f0/2
Switch(config-if)#switchport mode access !设置接口模式为接入模式
```

```

Switch(config-if)#switchport access vlan 10      !把接口加入 vlan 10
Switch(config-if)#exit
Switch(config-if)#in range f0/3-4               !进入接口组 f0/3-4
Switch(config-if-range)#switchport mode access  !设置接口模式为接入模式
Switch(config-if-range)#swaccvlan 20            !把接口加入 vlan 20

```

步骤 5：使用 show-vlan 命令验证 VLAN，如图 2-2-3 所示。

```

Switch#show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                           Gig0/1, Gig0/2
10   caiwubu                active    Fa0/1, Fa0/2
20   gongchengbu            active    Fa0/3, Fa0/4
1002 fddi-default            act/unsup
1003 token-ring-default    act/unsup
1004 fddinet-default        act/unsup
1005 trnet-default          act/unsup

```

图 2-2-3 验证 VLAN

步骤 6：测试网络的连通性。

(1) 在 PC1 上 ping PC2 的 IP 地址 192.168.1.12，网络是连通的，说明同一 VLAN 中的计算机能够互相通信，如图 2-2-4 所示。

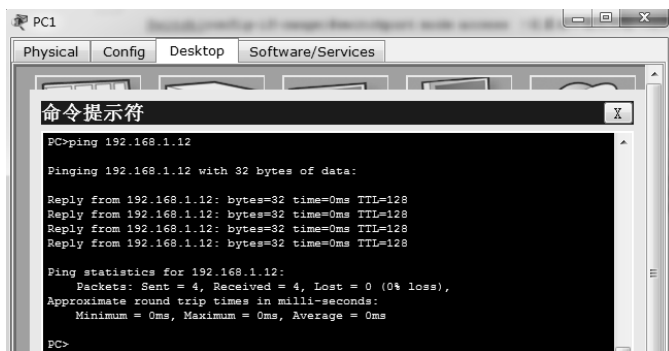


图 2-2-4 连通性测试效果图（一）

(2) 在 PC1 上 ping PC3 的 IP 地址 192.168.1.13，网络是不通的，说明不同 VLAN 中的计算机不能互相通信，如图 2-2-5 所示。

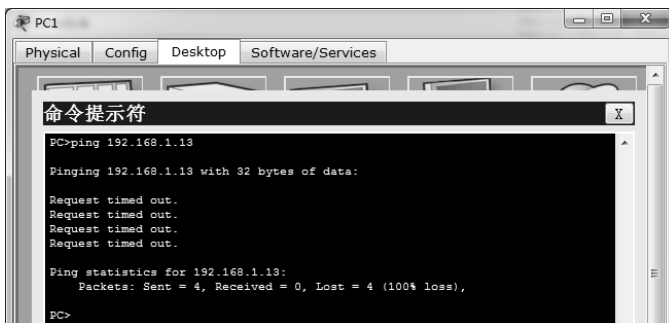


图 2-2-5 连通性测试效果图（二）



小贴士

VLAN 操作命令有如下几个。

创建 VLAN: VLAN [VLAN id] (如 VLAN10)。

删除 VLAN: no VLAN [VLAN id] (如 no VLAN10)

除了用户创建的 VLAN 之外, 还有系统自带的 VLAN, 如 VLAN1、VLAN1001 ~ VLAN1005, 这些 VLAN 是无法删除的。

默认情况下, 交换机所有端口都属于 VLAN1, 如果需要加入其他 VLAN, 则需要用命令 switchport access vlan<id>将端口显式地添加到 VLAN 中。

分组添加的方法: 连续的端口用 range 包括, 不连续的端口用逗号隔开, 格式如下。

```
Switch(config)#interface range fastEthernet 0/3 - 6,fastEthernet 0/10 ! 进入端口组
Switch(config-if-range)#switchport access vlan 20
```

删除一个 VLAN 后, VLAN 中的接口无法访问, 也不能自动加入 VLAN 1, 除非手动把这些接口加入其他 VLAN。

相关知识

1. 交换机与广播域

交换机可以根据帧中的目的 MAC 地址, 将消息流从一个端口转发到另一个端口。交换机根据 MAC 地址来传送流量。每台交换机都在被称为内容可寻址存储器 (CAM) 的高速内存中维护着一张 MAC 地址表。每次启动交换机时, 它都会使用传入帧的源 MAC 地址, 以及该帧进入交换机时所使用的端口号来重新创建 MAC 地址表, 如在图 2-2-6 中, 交换机创建的 MAC 地址表如表 2-2-2 所示。

表 2-2-2 交换机 MAC 地址表

Fa0/1	Fa0/2	Fa0/3	Fa0/4
0001.C9B0.578C	00E0.F996.75EA	0001.6362.8A7C	0030.A30B.6955

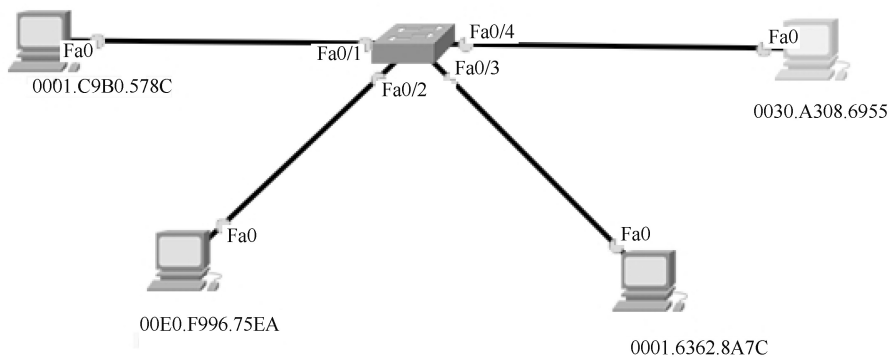


图 2-2-6 交换机 MAC 地址表

当单播帧进入端口时, 交换机会找出该帧内的源 MAC 地址, 然后在 MAC 地址表中搜索与该地址匹配的条目。如果源 MAC 地址尚未存在于表中, 交换机会将该 MAC 地址和端口号添加到表中, 并设置老化计时器。如果源 MAC 地址已存在于表中, 则交换机会重置其老化计时器。

然后, 交换机会在表中查找目的 MAC 地址。如果能找到, 则交换机将帧从相应的端口

转发出去。如果找不到，则交换机会向每个活动端口泛洪该帧，但接收该帧的端口除外。

如果收到广播帧，则交换机会像收到未知目的 MAC 地址时一样，将其泛洪到所有活动接口。所有收到该广播的设备便构成了广播域。相连接的交换机越多，广播域的规模就越大。

VLAN 技术实现了广播域的划分，使广播不会在不同 VLAN 间转发。

在交换机上可使用 `show mac-address-table` 命令来查看 MAC 地址表，本任务中划分了 3 个 VLAN，查看到的 MAC 地址表如图 2-2-7 所示。

```
Switch#show mac-address-table
```

MAC Address Table			
VLAN	MAC Address	Type	Ports
10	0004.9a35.bab3	DYNAMIC	Fa0/1
10	00d0.bc87.89d0	DYNAMIC	Fa0/2
20	0030.a3c6.a531	DYNAMIC	Fa0/6
20	00e0.a366.46bd	DYNAMIC	Fa0/7
30	0007.ecbc.8c98	DYNAMIC	Fa0/12
30	0030.a3d1.1848	DYNAMIC	Fa0/11

图 2-2-7 查看 MAC 地址表

学习小结

本任务介绍了在一台交换机上如何划分 VLAN，所有计算机设置了同一个网段的 IP 地址，只有相同 VLAN 的 PC 可以相互通信，不同 VLAN 的 PC 不能通信。通过 VLAN 的划分，可以实现广播域的控制。

任务 2 交换机间相同 VLAN 通信

同一台交换机上同一 VLAN 内 PC 可以通信，不同 VLAN 被隔离。但由于网络规模的增大或地域范围的限制，同一 VLAN 的用户可能跨接在不同交换机上，需要配置跨交换机链路实现交换机间相同 VLAN 的通信。

学习情境

海成公司有财务部、市场部等部门，其中在不同楼层内都有财务部和市场部的员工计算机，为了使公司的管理更加安全与便捷，公司的领导想让管理员组建公司局域网，使各个部门内部的主机之间的业务往来可以通信，但部门之间基于安全考虑，禁止部门之间互相访问。

情境分析

通过划分 VLAN 使得财务部和市场部之间不可以自由访问，但部门内的计算机分布在不同楼层的交换机上，又要互相访问，这就要使用 802.1Q 进行跨交换机的相同部门的访问，即在两台交换机之间开启 Trunk 进行通信。

所需设备：

- (1) Cisco Catalyst 2960 交换机 2 台。
- (2) PC 4 台。



(3) Console 线 1 条。

(4) 直通线 4 条。

(5) 交叉线 1 条。

任务拓扑结构如图 2-2-8 所示。

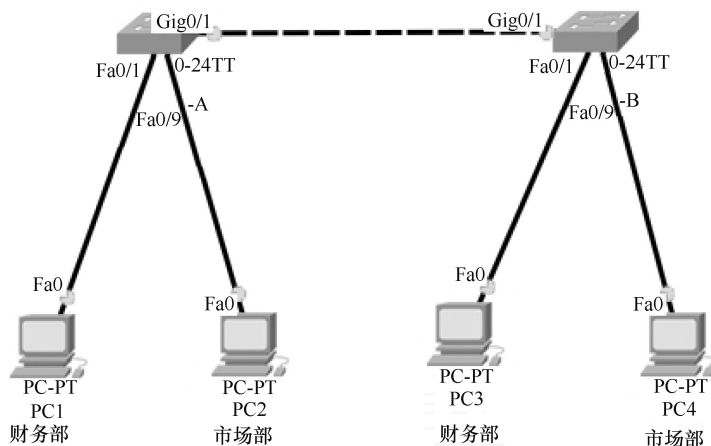


图 2-2-8 跨交换机相同 VLAN 的通信拓扑

交换机的 VLAN 划分及其参数设置如表 2-2-3 所示。

表 2-2-3 交换机 VLAN 划分及其参数设置

设 备	端 口 成 员	IP 地 址	子 网 掩 码	备 注
Switch-A 的 VLAN 10	1~5	无	无	无
Switch-A 的 VLAN 20	6~10	无	无	无
Switch-A	G0/1 (Trunk)	无	无	无
Switch-B 的 VLAN 10	1~5	无	无	无
Switch-B 的 VLAN 20	6~10	无	无	无
Switch-B	G0/1 (Trunk)	无	无	无
PC1	Switch-A 的 fa0/1	192.168.1.10	255.255.255.0	财务部
PC2	Switch-A 的 fa0/6	192.168.1.20	255.255.255.0	市场部
PC3	Switch-B 的 fa0/1	192.168.1.30	255.255.255.0	财务部
PC4	Switch-B 的 fa0/6	192.168.1.40	255.255.255.0	市场部

步骤实现

步骤 1：按照图 2-2-8 连接网络拓扑结构。

步骤 2：按照表 2-2-3 配置计算机的 IP 地址和子网掩码。

步骤 3：给交换机 A 设置名称，划分 VLAN 10 和 VLAN 20，并分配相应的端口。

```
Switch>en
Switch#conf t
switch(config)#hostname Switch-A      ! 交换机命名为 Switch-A
Switch-A(config)#vlan 10              ! 创建 vlan 10
Switch-A(config-vlan)#name caiwubu    ! 命名为 caiwubu
```

```

Switch-A(config-vlan)#exit
Switch-A(config)#vlan 20                                !创建 vlan 20
Switch-A(config-vlan)#name shichangbu                   !命名为 shichangbu
Switch-A(config-vlan)#exit
Switch-A(config)#in range f0/1-5                       !进入接口组 f0/1-5
Switch-A(config-if-range)#sw acc vlan 10                !把接口加入 vlan 10
Switch-A(config-if-range)#exit
Switch-A(config)#in range f0/6-10                      !进入接口组 f0/6-10
Switch-A(config-if-range)#sw access vlan 20             !接口加入 vlan 20
Switch-A(config-if-range)#exit
Switch-A(config)#end
Switch-A#

```

步骤 4: 给交换机 B 设置名称, 划分 VLAN 10、VLAN 20, 并分配相应的端口。

```

Switch>en
Switch#conf t
Switch(config)#hostname Switch-B                       !定义主机名为 Switch-B
Switch-B(config)#vlan 10                                !创建 vlan 10
Switch-B(config-vlan)#name student                     !命名为 student
Switch-B(config-vlan)#exit
Switch-B(config)#vlan 20                                !创建 vlan 20
Switch-B(config-vlan)#name teacher                     !命名为 teacher
Switch-B(config-vlan)#exit
Switch-B(config)#in range f0/1-5                       !进入接口组 f0/1-5
Switch-B(config-if-range)#sw acc vlan 10               !把接口加入 vlan 10
Switch-B(config-if-range)#exit
Switch-B(config)#in range f0/6-10                      !进入接口组 f0/6-10
Switch-B(config-if-range)#sw access vlan 20            !把口加入 vlan 20
Switch-B(config-if-range)#exit
Switch-B(config)#end
Switch-B#

```

步骤 5: 验证交换机 A 的 VLAN 配置, 如图 2-2-9 所示。

```
Switch-A#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/2
10	caiwubu	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
20	shichangbu	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

图 2-2-9 验证交换机 A 的 VLAN 配置



步骤 6：验证交换机 B 的 VLAN 配置，如图 2-2-10 所示。

```
Switch-B#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/16, Fa0/17, Fa0/18 Fa0/19, Fa0/20, Fa0/21, Fa0/22 Fa0/23, Fa0/24, Gig0/2
10 caiwubu	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5
20 shichangbu	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
1002 fddi-default	act/unsup	
1003 token-ring-default	act/unsup	
1004 fddinet-default	act/unsup	
1005 trnet-default	act/unsup	

图 2-2-10 验证交换机 B 的 VLAN 配置

步骤 7：测试网络的连通性。在 PC1 上 ping PC3 和 PC4 的 IP 地址 192.168.1.30、192.168.1.40，网络是不通的，如图 2-2-11 所示。

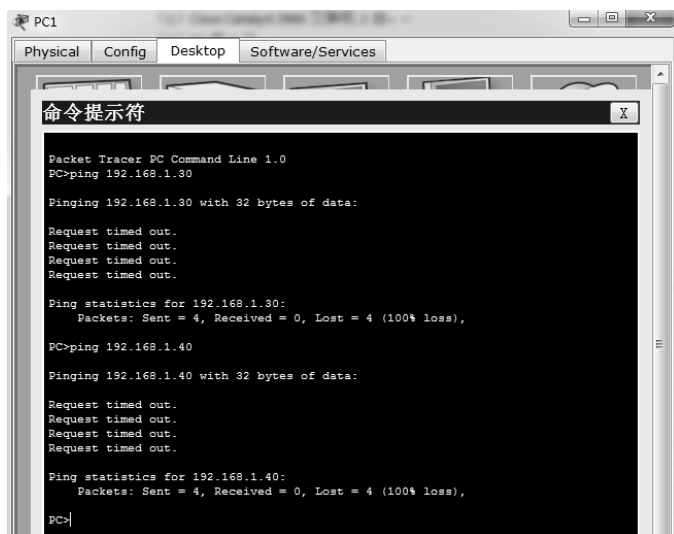


图 2-2-11 连通性测试效果图（一）



小贴士

说明跨交换机的相同 VLAN 的计算机无法互相通信，主要原因是没有配置 Trunk。

步骤 8：设置交换机 A 的 Trunk 端口。

```
Switch-A#conf t
Switch-A(config)#int g0/1
Switch-A(config-if)#switchport mode trunk
```

步骤 9：设置交换机 B 的 Trunk 端口。

```
Switch-B#conf t
Switch-B(config)#int g0/1
Switch-B(config-if)#switchport mode trunk
```

步骤 10: 验证交换机 A 的配置。

```
Switch-A# show int g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk ! 已经是 Trunk 模式
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL ! 允许所有 vlan 通过
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Switch-A#
```

步骤 11: 验证交换机 B 的配置。

```
Switch-B#show int g0/1 switchport
Name: Gig0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
```



```
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Switch-B#
```

步骤 12: 测试网络的连通性。在 PC1 上 ping PC3 的 IP 地址 192.168.1.30, 网络是连通的, 表明交换机之前的 Trunk 链路已经成功建立; ping PC4 的 IP 地址 192.168.1.40, 网络不通, 表明不同 VLAN 间无法通信, 如图 2-2-12 所示。

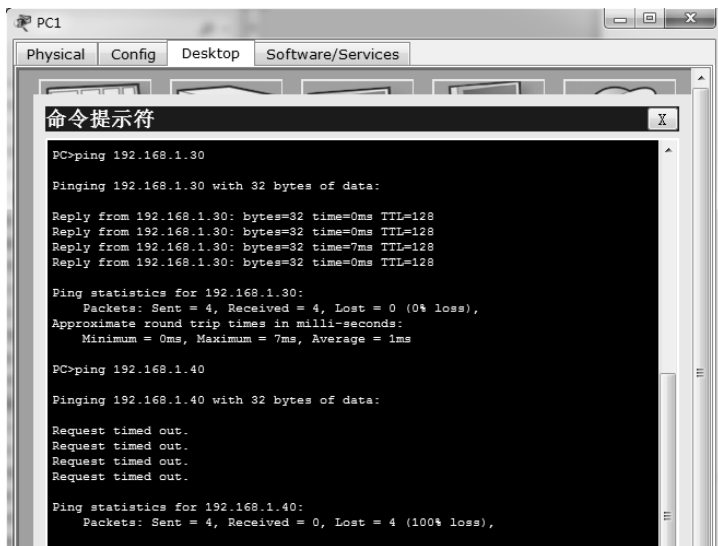


图 2-2-12 连通性测试效果图（二）



小贴士

要将某个交换机端口从 VLAN 10 中删除, 将端口重新分配给 VLAN 1, 可以在接口配置模式下使用 `no switchport access vlan` 命令。

静态接入端口只能拥有一个 VLAN。通过使用 Cisco IOS 软件, 不需要将端口从 VLAN 中删除, 即可将其分配给其他 VLAN。当将静态接入端口重新分配给现有的 VLAN 时, 该 VLAN 会自动从原来的端口上删除。

也可以在特权执行模式下使用 “`delete flash:vlan.dat`” 命令来删除整个 `vlan.dat` 文件。交换机重新加载后, 先前配置的 VLAN 将不存在。这种方法能有效地将交换机的 VLAN 配置还原为 “出厂默认设置”。

删除 VLAN 之前, 务必将所有成员端口重新分配给其他 VLAN。在删除 VLAN 后, 任何未转移到活动 VLAN 的端口都将无法与其他站点通信。

相关知识

Cisco 交换机的端口状态有 3 种模式: `access`、`trunk` 和 `auto`, 分别对应接入模式、中继模

式和自动协商模式，默认为 auto 模式。如果某个端口连接 PC，则应该配置为 access 模式，即把端口分配给某个 VLAN。如果交换机端口连接的是另一台交换机，而且存在多个 VLAN 需要跨交换机通信，则此端口需要承载多个 VLAN 的数据，应设置为 trunk 模式。当某端口连接 Cisco 交换机时，如果端口处于 auto 状态，则会与链路对端口自动协商状态。此例中两台 Cisco 交换机互连，一端配置为 trunk 后，另一端默认为 auto 状态，则协商后自动转换为 trunk，所以不需要手工配置。如果 Cisco 交换机与非 Cisco 交换机互连，则不能自动协商，需要在两端手工配置为 trunk 状态。

学习小结

本任务介绍了在一个网络上存在两个或两个以上的交换机互连时，且交换机都进行了相同的 VLAN 配置，设置交换机相连的端口为 Trunk 类型，并允许相应的 VLAN 通过，可以实现交换机之间相同 VLAN 上的计算机的相互通信。

任务 3 三层交换机的配置

三层交换机即内置了路由功能的交换机，在转发数据帧的同时，还可以在不同网段之间路由数据包。在交换式局域网中，三层交换机可以配置多个虚拟 VLAN 接口（SVI）作为 VLAN 内 PC 设备的网关，同时转发数据包，实现不同 VLAN 之间的通信。

学习情境

海成公司由于业务的需要，公司内部办公系统需要控制不同业务部门之间的访问。公司准备用一台 Cisco Catalyst 3560 交换机作为路由设备来实现不同部门之间的互访需求。

情境分析

将不同业务部门划分到不同 VLAN，管理更为合理、安全，但有时又需要部门间相互通信，这可通过三层交换机设备来实现。

所需设备：

- (1) Cisco Catalyst 3560 交换机 1 台。
- (2) PC 2 台。
- (3) Console 线 1 条。
- (4) 直通线 2 条。

任务拓扑结构如图 2-2-13 所示。

网络参数设置如表 2-2-4 所示。

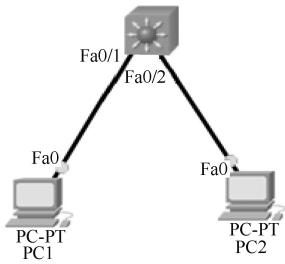


图 2-2-13 三层交换机的配置

表 2-2-4 网络参数设置

设 备	端 口	IP 地址	子网掩码	网 关
VLAN 10	1~2	192.168.10.1	255.255.255.0	无
VLAN 20	3~4	192.168.20.1	255.255.255.0	无
PC1	1	192.168.10.10	255.255.255.0	192.168.10.1
PC2	3	192.168.20.10	255.255.255.0	192.168.20.1

步骤实现

步骤 1：按照图 2-2-13 连接网线拓扑结构。

步骤 2：按照表 2-2-4 配置计算机的 IP 地址和子网掩码。



步骤 3：在三层交换机上设置主机名称，创建 VLAN 并添加端口。

```
Switch>en
Switch#conf t
Switch(config)#hostname Switch-A
Switch-A(config)#vlan 10
SWITCH-A(config-vlan)#exit
SWITCH-A(config)#vlan 20
SWITCH-A(config-vlan)#exit
SWITCH-A(config)#int range f0/1-2
SWITCH-A(config-if-range)#switchport access vlan 10
SWITCH-A(config-if-range)#exit
SWITCH-A(config-if-range)#in range f0/3-4
SWITCH-A(config-if-range)#switchport access vlan 20
SWITCH-A(config-if-range)#exit
SWITCH-A(config)#end
```

步骤 4：在交换机-A 上配置 VLAN 10 和 VLAN 20 的 IP 地址。

```
SWITCH-A(config)#int vlan 10      !进入 vlan 10 接口
SWITCH-A(config-if)#ip add 192.168.10.1 255.255.255.0 !给 vlan 10 配置 IP 地址
SWITCH-A(config-if)#no shutdown      !打开 vlan 10 接口
SWITCH-A(config-if)#exit
SWITCH-A(config)#int vlan 20
SWITCH-A(config-if)#ip add 192.168.20.1 255.255.255.0 !给 vlan 20 配置 IP 地址
SWITCH-A(config-if)#no shutdown
SWITCH-A(config-if)#end
SWITCH-A#
```

步骤 5：开启三层交换机的路由功能，交换机工作在路由模式下，才可设置 VLAN 间路由。

```
SWITCH-A>en
SWITCH-A#conf t
SWITCH-A(config)#ip routing      !开启三层交换机的路由功能
SWITCH-A(config)#end
SWITCH-A#
```

步骤 6：验证交换机 A 的配置。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.10.0/24 is directly connected, Vlan10
```

```
C 192.168.20.0/24 is directly connected, Vlan20
Switch-A#
```

步骤 7：测试 PC 连通性。在 PC 1 上 ping PC 2 的 IP 地址 192.168.20.10，网络已连通，如图 2-2-14 所示。

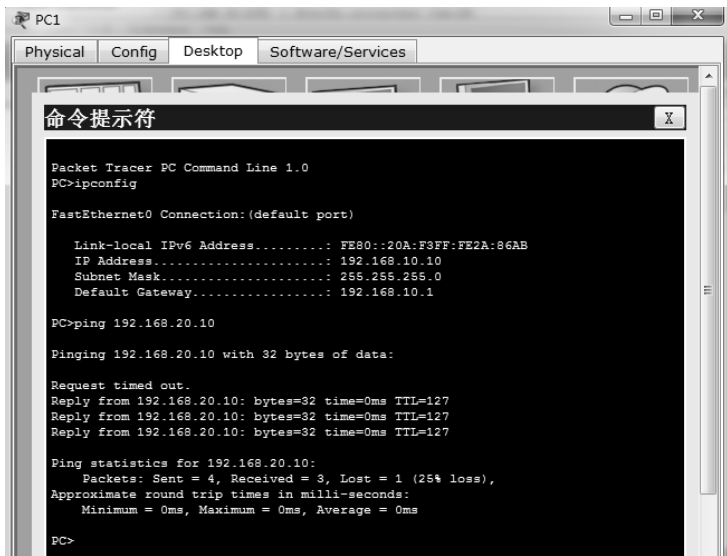


图 2-2-14 连通性测试效果图

相关知识

三层交换机与路由器的区别：三层交换机也具有“路由”功能，它与传统路由器的路由功能总体上是一致的，但是，三层交换机与路由器还存在着相当大的本质区别。

1. 主要功能不同

虽然三层交换机与路由器都具有路由功能，但不能把它们等同起来，正如现在许多网络设备同时具备多种传统网络设备功能一样，如现在有许多宽带路由器不仅具有路由功能，还提供了交换机端口、硬件防火墙功能，但不能把它与交换机或者防火墙等同起来。因为这些路由器的主要功能还是路由，其他功能只是其附加功能，其目的是使设备适用面更广、更加实用。这里的三层交换机也一样，它仍是交换机产品，但它是具备了一些基本路由功能的交换机，它的主要功能仍是数据交换。也就是说，它同时具备了数据交换和路由转发两种功能，但其主要功能是数据交换；而路由器仅具有路由转发这一种主要功能。

2. 主要适用的环境不同

三层交换机的路由功能通常比较简单，因为它所面对的主要是简单的局域网连接。正因如此，三层交换机的路由功能通常比较简单，路由路径远没有路由器那样复杂。它在局域网中的主要用途是提供快速数据交换功能，满足局域网数据交换频繁的应用特点。

而路由器则不同，它的设计初衷是为了满足不同类型的网络连接，虽然也适用于局域网之间的连接，但它的路由功能更多地体现在不同类型网络之间的互连上，如局域网与广域网之间的连接、不同协议的网络之间的连接等，所以路由器主要用于不同类型的网络之间。它最主要的功能是路由转发，解决好各种复杂路由路径网络的连接是它的最终目的，所以路由



器的路由功能通常非常强大，不仅适用于同种协议的局域网间，更适用于不同协议的局域网与广域网间。它的优势在于选择最佳路由、负荷分担、链路备份及和其他网络进行路由信息的交换等。为了与各种类型的网络连接，路由器的接口类型非常丰富，而三层交换机则一般仅是同类型的局域网接口，非常简单。

3. 性能体现不同

从技术上讲，路由器和三层交换机在数据包交换操作上存在着明显区别。路由器一般由基于微处理器的软件路由引擎执行数据包交换，而三层交换机通过硬件执行数据包交换。三层交换机在对第一个数据流进行路由后，将产生一个 MAC 地址与 IP 地址的映射表，当同样的数据流再次通过时，将根据此表直接从二层通过而不是再次路由，从而消除了路由器进行路由选择而造成的网络延迟，提高了数据包转发的效率。同时，三层交换机的路由查找是针对数据流的，它利用缓存技术，很容易利用 ASIC 技术来实现，因此，可以大大节约成本，并实现快速转发。而路由器的转发采用了最长匹配的方式，实现复杂，通常使用软件来实现，转发效率较低。

正因如此，从整体性能上比较，三层交换机的性能要远优于路由器，非常适用于数据交换频繁的局域网；而路由器虽然路由功能非常强大，但它的数据包转发效率远低于三层交换机，更适用于数据交换不是很频繁的不同类型网络的互连，如局域网与互联网的互连。如果把路由器，特别是高档路由器用于局域网，则在相当大的程度上是一种浪费（就其强大的路由功能而言），而且不能很好地满足局域网通信性能需求，影响子网间的正常通信。

三层交换机在实际应用中，经常上连路由器等出口设备，可以把上连口启用三层功能，配置 IP 地址，参与路由。

三层交换机物理接口配置 IP 地址时，需要在接口模式下先启用三层功能，才可以配置 IP 地址，命令如下。

```
Switch(config)#interface f0/24
Switch(config-if)#no switchport
Switch(config-if)#ip address 10.0.0.1 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#end
Switch#
```

学习小结

本任务介绍了如何在三层交换机上实现不同部门之间的通信，在二层交换机配置 VLAN 后，只能实现相同 VLAN 的通信，如果想实现 VLAN 间通信，则必须借助于三层设备（三层交换机或路由器），路由器实现 VLAN 间通信，将在后面的项目中进行介绍。

实训 3 交换机的常用技术

交换机在现代高速网络中应用非常广泛，相关的应用除了最常用的 VLAN 技术外，还包括链路聚合、VTP 协议、生成树技术、DHCP 服务和冗余网关 HSRP 等。这 5 项技术分别对应到如下 5 个任务来学习。

任务 1 交换机的链路聚合技术。

任务 2 交换机的 VTP 技术。

- 任务 3 交换机的生成树技术。
- 任务 4 交换机的 DHCP 服务。
- 任务 5 交换机的 HSRP 技术。

任务 1 交换机的链路聚合技术

链路聚合又称为端口汇聚，是指两台交换机之间在物理上将两个或多个端口连接起来，将多条链路聚合成一条逻辑链路，从而增大链路带宽，多条物理链路之间能够相互冗余备份。

学习情境

海成公司的局域网已经投入使用，功能上完全满足了公司办公和业务需求。但有时出现上网高峰期访问服务器或外网时速度降低，影响办公效率的情况。网络管理员需要想办法增大交换机上连接口的带宽。

情境分析

链路聚合技术可以将交换机与核心交换机之间的多个端口并行连接，多条链路聚合成一条链路，从而增大链路带宽，解决交换网络中因带宽引起的网络瓶颈问题，其中任意一条链路断开，都不会影响其他链路的正常转发数据。

所需设备：

- (1) Cisco Catalyst 2960 交换机 2 台。
- (2) PC 2 台
- (3) Console 线 1 条。
- (4) 直通线 2 条。
- (5) 交叉线 2 条。

任务拓扑结构如图 2-3-1 所示。

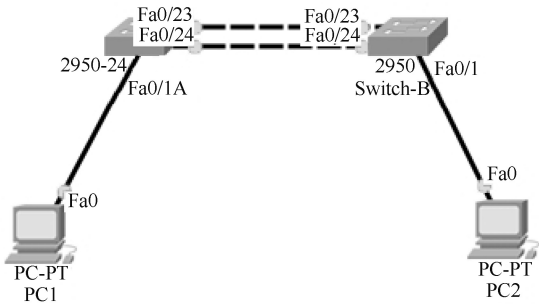


图 2-3-1 交换机链路聚合拓扑图

PC IP 地址的分配如表 2-3-1 所示。

表 2-3-1 PC IP 地址分配表

PC 编号	所属 VLAN	IP 地址	子网掩码
PC1	10	192.168.1.10	255.255.255.0
PC2	20	192.168.1.20	255.255.255.0

步骤实现

步骤 1：按照图 2-3-1 连接拓扑结构。



步骤 2：按照表 2-3-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：设置交换机 A 的名称和划分 VLAN 10，并将 fa0/1 加入到 VLAN 10 中。

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-A      !定义主机名为 Switch-A
Switch-A(config)#vlan 10              !划分 vlan 10
Switch-A(config-vlan)#exit
Switch-A(config)#in f0/1
Switch-A(config-if)#switchport acc vlan 10 !将接口 f0/1 加入 vlan 10
Switch-A(config-if)#end
Switch-A#
```

步骤 4：设置交换机 B 的名称和划分 VLAN 10，并将 fa0/1 加入到 VLAN 10 中。

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-B
Switch-B(config)#vlan 10
Switch-B(config-vlan)#exit
Switch-B(config)#in f0/1
Switch-B(config-if)#sw
Switch-B(config-if)#switchport acc
Switch-B(config-if)#switchport access vlan 10
Switch-B(config-if)#end
Switch-B#
```

步骤 5：在交换机 A 上配置聚合端口，端口 f0/23、24 为聚合口，并开启中继模式。

```
Switch-A(config)#in range f0/23-24      !进入接口组 f0/23-24
Switch-A(config-if-range)#channel-group 1 mode on !定义聚合端口 1
Switch-A(config-if-range)#exit
Creating a port-channel interface Port-channel 1 !系统提示：聚合端口号建立
Switch-A(config-if-range)#exit
Switch-A(config)#in port-channel 1      !进入聚合口 1
Switch-A(config-if)#switchport mode trunk !开启中继模式
Switch-A(config-if)#end
Switch-A#
```

步骤 6：在交换机 B 上配置聚合端口，端口 f0/23、24 为聚合口，并开启中继模式。

```
Switch-B(config)#in range f0/23-24      !进入接口组 f0/23-24
Switch-B(config-if-range)#channel-group 1 mode on !定义聚合口 1
Switch-B(config-if-range)#
Creating a port-channel interface Port-channel 1
Switch-B(config-if-range)#exit          !退出接口模式
Switch-B(config)#in port-channel 1      !进入聚合口 1
```

```
Switch-B(config-if)#switchport mode trunk      !开启中继模式
Switch-B(config-if)#end
Switch-B#
```

步骤 7: 在交换机 A 上验证端口聚合。

```
Switch-A#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1      !正在使用的聚合口:1 个
Number of aggregators:          1      !聚合口总数: 1 个

Group Port-channel Protocol Ports
-----+-----+-----+-----
-----
1      Pol(SU)        -      Fa0/23(P) Fa0/24(P)
```

步骤 7: 在交换机 B 上验证端口聚合。

```
Switch-B#show etherchannel summary
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       U - in use        f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group Port-channel Protocol Ports
-----+-----+-----+-----
-----
1      Pol(SU)        -      Fa0/23(P) Fa0/24(P)
```



步骤 8：测试 PC 连通性。在 PC 1 上测试与 PC 2 的连通性，如图 2-3-2 所示。

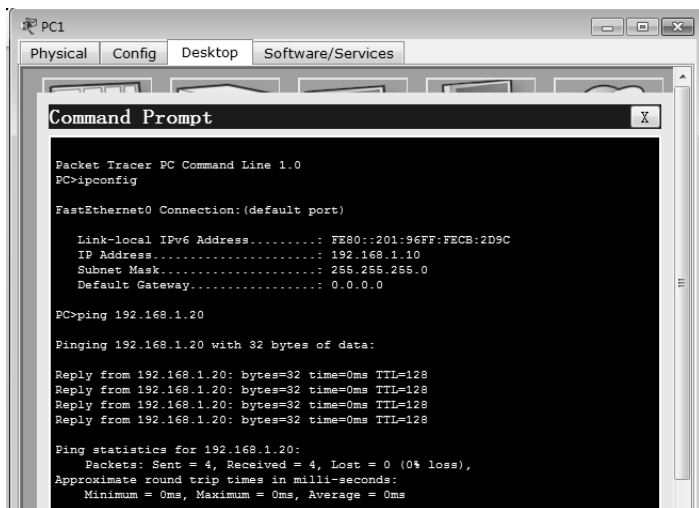


图 2-3-2 测试 PC 的连通性

步骤 9：改变拓扑结构重新测试。把聚合口的连线去掉一条，重新测试连通性。此时会发现，去掉一条连线后，PC 连通性没有受到影响，如图 2-3-3 所示。

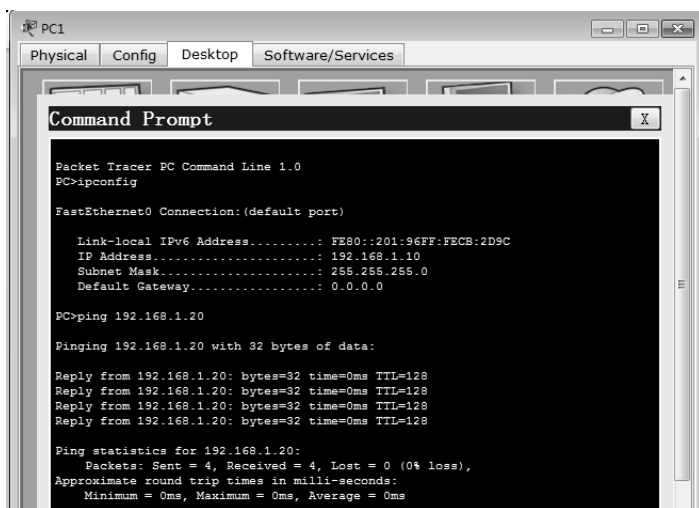


图 2-3-3 测试 PC1 与 PC2 的连通性



小贴士

- (1) 在设置交换机的端口聚合时应选择偶数数目的端口，如 2 个、4 个、8 个等。
- (2) 选择的端口必须是连续的。
- (3) 端口汇聚组应设置为 Trunk 模式。

相关知识

EtherChannel 技术最初是由思科公司开发的，是一种将多个快速以太网或千兆以太网端口集合到一个逻辑通道中的 LAN 交换机到交换机技术。当配置 EtherChannel 时，所产生的虚拟接口称为端口通道。物理接口捆绑在一起称为一个端口通道接口。

1. EtherChannel 技术的优点

大多数配置任务可以在 EtherChannel 接口（而不是在每个端口）上完成，这能确保链路中的配置一致。

EtherChannel 依赖现有交换机端口，无需将链路升级到拥有更高带宽的更快、更昂贵的连接。

负载均衡在属于同一 EtherChannel 的链路之间进行。根据硬件平台，可以实施一个或多个负载均衡方法。这些方法包括物理链路上源 MAC 地址到目的 MAC 地址负载均衡或源 IP 地址到目的 IP 地址负载均衡。

EtherChannel 创建的聚合被视为一个逻辑链路。当两台交换机之间存在多个 EtherChannel 包时，STP 可能会阻塞其中一个包，以防止交换环路。当 STP 阻塞其中一个冗余链路时，它会阻塞整个 EtherChannel。这将阻塞属于此 EtherChannel 链路的所有端口。如果只有一个 EtherChannel 链路，则 EtherChannel 中的所有物理链路都有效，因为 STP 只看到一条（逻辑）链路。

EtherChannel 可提供冗余，因为总体链路被视为一个逻辑连接。此外，通道内一个物理链路的丢失不会造成拓扑的变化，因此不需要重新计算生成树。假设至少存在一个物理链路，则 EtherChannel 将保持正常运行，虽然其总体吞吐量会因 EtherChannel 中的链路丢失而减少。

2. EtherChannel 的指导原则和限制

EtherChannel 支持：所有模块上的所有以太网接口都必须支持 EtherChannel，而不要求接口在物理上连续或位于同一模块。

速度和双工：将 EtherChannel 中的所有接口配置为以相同速度并在相同双工模式下运行。

VLAN 匹配：必须将 EtherChannel 中的所有接口分配到相同 VLAN 中，或配置为 Trunk。

VLAN 范围：在中继 EtherChannel 中的所有接口上，EtherChannel 都支持相同的 VLAN 允许范围。如果 VLAN 的允许范围不同，那么即使设置为自动或期望的模式，接口也不会形成 EtherChannel。

如果必须更改这些设置，可在端口通道接口配置模式下修改。当配置了端口通道接口后，任何应用于端口通道接口的配置都会影响各个接口。但是，应用于单个接口的配置不会影响端口通道接口。因此，对属于 EtherChannel 链路的接口进行配置更改可能会导致接口兼容性问题。

学习小结

当连接好设备时，在交换机互连的两条链路中，若有一条链路标志是黄色的，则表示该链路处于关闭状态，此时两台交换机之间并没有实现链路聚合功能。当做完以上配置时，再次检查网络拓扑图可以发现，这时交换机互连的两条链路的标记都是绿色，当交换机之间的一条链路断开时，PC 1 与 PC 2 仍能互相通信。

任务 2 交换机的 VTP 技术

虚拟局域网干道协议（VLAN Trunk Protocol, VTP）即 VLAN 的中继协议。VTP 通过网络保持 VLAN 配置的统一性。VTP 实现了系统化管理，方便管理员增加、删除和调整的



VLAN 操作。只要把交换机加入到同一个 VTP 域中，工作在服务器模式的交换机会自动地将 VLAN 配置信息向网络中其他的交换机广播，VTP 客户端会自动学习 VTP 服务器上的 VLAN 信息。此外，VTP 还减小了那些可能导致安全问题的配置，便于管理。

学习情境

海成公司的局域网在使用过程中，由于业务的改变经常需要增加或删除 VLAN，由于交换机数量较多，位置分散，为能够保证 VLAN 配置的统一性，管理员需要花费较多的时间来管理。为解决这一问题，可使用 VTP 技术。

情境分析

对于多台交换机的 VLAN 管理，使用 VTP 技术最为合适。设置核心层交换机为 VTP 服务器，并规划相应的 VLAN。接入层交换机为 VTP 客户机，使它们实现 VLAN 的中继，自动创建与 VTP 服务器相同的 VLAN 规划。配置交换机互连端口为 Trunk 类型，规划接入层 VLAN 的端口分配，最终实现全网互通。

所需设备：

- (1) Cisco Catalyst 3560 交换机 1 台。
- (2) Cisco Catalyst 2960 交换机 2 台。
- (3) PC 4 台。
- (4) Console 线 1 条。
- (5) 直通线 4 条。
- (6) 交叉线 2 条。

任务拓扑结构如图 2-3-4 所示。

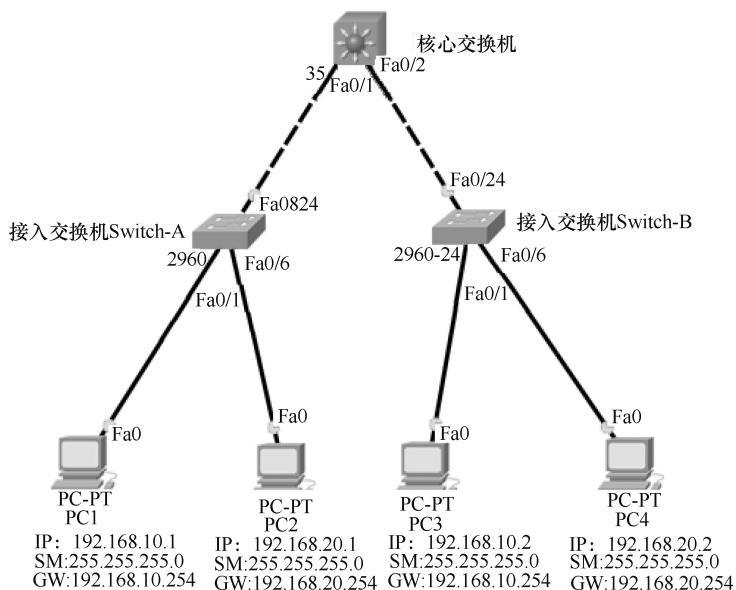


图 2-3-4 交换机 VTP 技术配置拓扑图

步骤实现

步骤 1：按照图 2-3-4，连接拓扑结构图，配置计算机的 IP 地址、子网掩码和网关。

步骤 2：配置核心交换机 C 的主机名称，将其设置为 VTP 服务器，设置 VTP 的域名与密码。

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-C
Switch-C(config)#vtp domain mydomain          !配置 VTP 域名为 mydomain
Changing VTP domain name from NULL to mydomain
Switch-C(config)#vtp mode server              !设置 VTP 模式为服务器模式
Device mode already VTP SERVER.
Switch-C(config)#vtp password cisco          !设置 VTP 密码为 cisco
Setting device VLAN database password to cisco
Switch-C(config)#

```

步骤 3: 配置接入交换机 A 的主机名称, 将其设置为 VTP 客户端, 域名和密码与 VTP 服务器相同。

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-A
Switch-A(config)#vtp domain mydomain          ! VTP 域名与核心交换机保持一致
Changing VTP domain name from NULL to mydomain
Switch-A(config)#vtp password cisco          !设置 VTP 密码为 cisco
Setting device VLAN database password to cisco
Switch-A(config)#vtp mode client             !设置 VTP 模式为客户端模式
Setting device to VTP CLIENT mode.
Switch-A(config)#

```

步骤 4: 配置接入交换机 B 的主机名称, 将其设置为 VTP 客户端, 域名和密码与 VTP 服务器相同。

```

Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-B
Switch-B(config)#vtp domain mydomain          ! VTP 域名与核心交换机保持一致
Changing VTP domain name from NULL to mydomain
Switch-B(config)#vtp password cisco          !设置 VTP 密码为 cisco
Setting device VLAN database password to cisco
Switch-B(config)#vtp mode client             !设置 VTP 模式为客户端模式
Setting device to VTP CLIENT mode.
Switch-B(config)#

```

步骤 5: 在核心交换机 C 上规划 VLAN 并配置网关, 启动路由功能。

```

Switch-C(config)#vlan 10                      !定义 vlan 10
Switch-C(config-vlan)#exit
Switch-C(config)#vlan 20                      !定义 vlan 20
SWITCH-C(config-vlan)#exit
SWITCH-C(config)#in vlan 10                  !为 vlan 10 配置网关, 使其可与 vlan 外部通信
SWITCH-C(config-if)#ip add 192.168.10.254 255.255.255.0
SWITCH-C(config-if)#no shutdown
SWITCH-C(config-if)#in vlan 20              !为 vlan 20 配置网关, 使其可与 vlan 外部通信

```




```
SWITCH-C(config-if)#ip add 192.168.20.254 255.255.255.0
SWITCH-C(config-if)#no shutdown
SWITCH-C(config-if)#exit
SWITCH-C(config)#ip routing
```

!开启三层交换机的路由功能

步骤 6：配置各交换机上的中继链路。

```
SWITCH-A(config)#in f0/24
SWITCH-A(config-if)#sw mode trunk
SWITCH-A(config-if)#
SWITCH-B(config)#in f0/24
SWITCH-B(config-if)#sw mode trunk
SWITCH-B(config-if)#
SWITCH-C(config)#in f0/1
SWITCH-C(config-if)#sw mode trunk
SWITCH-C(config-if)#in f0/2
SWITCH-C(config-if)#sw mode trunk
```

步骤 7：查看 VTP 客户端交换机上的 VLAN 配置。可以看到，此时接入交换机上已经存在了两个 VLAN，即 VLAN 10 和 VLAN 20。

```
Switch-A#sh vlan
```

	VLAN Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Gig0/1 Gig0/2
10	VLAN0010	active	
20	VLAN0020	active	

步骤 8：在接入交换机 A 上把相应端口加入 VLAN。

```
Switch-A(config)#in range f0/1-5
Switch-A(config-if-range)#sw acc vlan 10
Switch-A(config-if-range)#in range f0/6-10
Switch-A(config-if-range)#sw acc vlan 20
Switch-A(config-if-range)#end
Switch-A#
```

步骤 9：在接入交换机 B 上把相应端口加入 VLAN。

```
Switch-B(config)#in range f0/1-5
Switch-B(config-if-range)#sw acc vlan 10
Switch-B(config-if-range)#in range f0/6-10
Switch-B(config-if-range)#sw acc vlan 20
Switch-B(config-if-range)#end
Switch-B#
```

步骤 10: 验证 PC 的连通性。在任意一台 PC 上测试与其他 PC 的连通性, 应该都是互通的。在 PC 1 上分别测试其与 PC 3、PC 4 的连通性, 结果如图 2-3-5 所示。

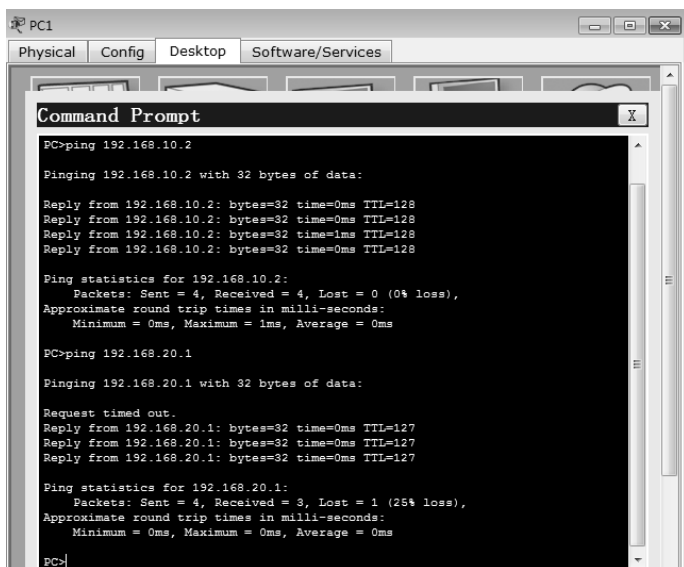


图 2-3-5 测试 PC 的连通性



小贴士

所有交换机的 VTP 域名一致、密码相同才能传输 VTP 消息。注意, VTP 域名、密码都是区分大小写的, 所以配置时要注意检查。

VTP 是思科公司开发的私有协议, 只能运行在思科公司的设备上, 不支持其他品牌的设备, 所以在多种品牌设备互连时, 不能使用 VTP 技术。

相关知识

1. VTP 的工作模式

VTP 中的交换机有 3 种工作模式: 服务器模式、客户端模式和透明模式。在 VTP 服务器上可以定义和删除 VLAN, 客户端交换机能够自动进行同步配置。工作在 VTP 透明模式的交换机不受影响, 可独立配置, 但是工作在 VTP 透明模式的交换机参与传输 VTP 域中的信息。

2. VTP 的状态及参数

Cisco IOS 命令 “show VTP status” 可显示 VTP 状态。输出信息显示交换机 Switch-A 默认为 VTP 服务器模式, 并且没有分配 VTP 域名。此输出还显示该交换机的最高可用 VTP 版本是第 2 版, 并且 VTP 第 2 版被禁用。在网络中配置和管理 VTP 时, 会经常用到 show VTP status 命令。下面简要说明 show VTP status 命令的参数。

VTP Version: 显示交换机可以运行的 VTP 版本。默认情况下, 交换机采用第 1 版, 但可以设置为第 2 版。

Configuration Revision: 交换机上的当前配置修订版号。后面将介绍更多有关修订版号的知识。

Maximum VLANs Supported Locally: 本地支持的最大 VLAN 数量。

Number of Existing VLANs: 现有 VLAN 的数量。



VTP Operating Mode: 可以是服务器、客户端或透明模式。

VTP Domain Name: 用于标识交换机管理域的名称。

VTP Pruning Mode: 显示修剪模式是启用还是禁用。

学习小结

本任务介绍了交换机 VTP 技术的应用，VTP 技术大大减轻了网络管理员对 VLAN 的管理操作，使网络管理员能方便地增加、删除和调整网络中的 VLAN 规划，并保持网络中 VLAN 规划的统一性。

任务 3 交换机的 STP 技术

网络的可靠性要求网络设备能够满足 7×24 小时的不间断工作，这就需要在网络中增加冗余的链路。生成树协议（Spanning Tree Protocol STP）技术使网络保持在一种无环、最优的工作状态，网络管理员可以基于 VLAN 流量调整生成树状态，是达到网络的负载均衡，使网络达到最佳工作效率。

学习情境

海成公司由于业务迅速发展和对网络可靠性的提高，增加了设备间的备份链路，希望使网络在不间断的情况下能达到最佳的工作效率。

情境分析

生成树技术可以在交换机网络中消除第二层环路，在网络出现故障时，能及时补充有效链路保障网络的可用性。在网络正常运行时，可以基于不同的 VLAN 进行转发，起到负载均衡的作用，提高网络的工作效率。

在两个交换机 Switch-A 和 Switch-B 上划分 VLAN 10 和 VLAN 20，将 PC 分别接入对应的 VLAN；在两个交换机上配置生成树协议，实现 VLAN 的负载均衡，使得 VLAN 10 的计算机由 Switch-A 转发，VLAN 20 的计算机通信时由 Switch-B 转发。

所需设备：

- (1) Cisco Catalyst 2960 交换机 2 台。
- (2) PC 4 台
- (3) Console 线 1 条。
- (4) 直通线 4 条。
- (5) 交叉线 2 条。

任务拓扑结构如图 2-3-6 所示。

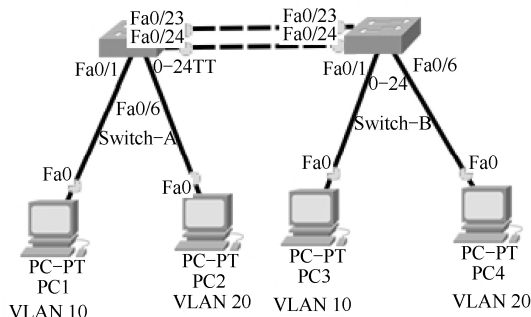


图 2-3-6 交换机 STP 技术配置拓扑图

PC 的 IP 地址配置如表 2-3-2 所示。

表 2-3-2 PC 的 IP 地址配置

PC 机编号	所属 VLAN	IP 地址	子网掩码
PC1	10	192.168.10.1	255.255.255.0
PC2	20	192.168.20.1	255.255.255.0
PC3	10	192.168.10.2	255.255.255.0
PC4	20	192.168.20.2	255.255.255.0

步骤实现

步骤 1：按照图 2-3-6 连接拓扑结构。

步骤 2：按照表 2-3-2 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置交换机 A 的主机名称，并划分 VLAN 10 和 VLAN 20，将 f0/1-5 划入 VLAN 10，f0/6-10 划入 VLAN 20。

```
Switch(config)#hostname Switch-A           !配置主机名
Switch-A(config)#vlan 10                   !创建 VLAN 10
Switch-A(config-vlan)#exit
Switch-A(config)#vlan 20                   !创建 VLAN 20
Switch-A(config-vlan)#exit
Switch-A(config)#in range f0/1-5           !将端口 1-5 加入 VLAN 10
Switch-A(config-if-range)#switchport access VLAN 10
Switch-A(config-if-range)#exit
Switch-A(config)#int range f0/6-10         !将端口 6-10 加入 VLAN 20
Switch-A(config-if-range)#switchport access vlan 20
Switch-A(config-if-range)#exit
Switch-A(config)#in range f0/23-24         !将交换机间互连端口为设置中继状态
Switch-A(config-if-range)#switchport mode trunk
```

步骤 4：配置交换机 B 的主机名称，并划分 VLAN 10 和 VLAN 20，将 f0/1-5 划入 VLAN 10，f0/6-10 划入 VLAN 20。

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-B
Switch-B(config)#vlan 10
Switch-B(config-vlan)#exit
Switch-B(config)#vlan 20
Switch-B(config-vlan)#exit
Switch-B(config)#in range f0/1-5
Switch-B(config-if-range)#switchport access vlan 10
Switch-B(config-if-range)#in range f0/6-10
Switch-B(config-if-range)#switchport access vlan 20
Switch-B(config-if-range)#exit
Switch-B(config)#in range f0/23-24         !将交换机间互连端口设置为中继状态
Switch-B(config-if-range)#switchport mode trunk
```



步骤 5：在 Switch-A 上启用生成树模式 **rapid-pvst**(为每 VLAN 快速生成树)。交换机上默认开启生成树协议，这里选择 **rapid-pvst**（RSTP）生成树协议，既可以达到快速收敛，又可以在每个 VLAN 上构建生成树，以达到负载均衡。

```
Switch-A(config)#spanning-tree mode ?
pvst          Per-Vlan spanning tree mode          !每个 VLAN 生成树
  rapid-pvst  Per-Vlan rapid spanning tree mode      !快速每个 VLAN 生成树
Switch-A(config)#spanning-tree mode rapid-pvst
```

步骤 6：验证在 Switch-B 上开启生成树模式 **rapid-pvst**（快速每个 VLAN 生成树）的结果。

```
Switch-B#show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp    !生成树协议版本为 rstp
  Root ID    Priority    32769          !根桥优先级（默认优先级为 32768+VLAN ID）
           Address      0000.0C84.1692   !根桥 MAC 地址
           Cost         19              !本地网桥到达根桥开销
           Port         23(FastEthernet0/23) !与根桥互连端口
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           !Hello 老化时间及转发延迟

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1) !本网桥优先级
           Address      00D0.FF65.029B          !本网桥 MAC 地址
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

Interface                Role      Sts      Cost      Prio.Nbr Type
-----
Fa0/24                   Altn BLK 19      128.24    P2p      !端口状态为阻塞，即不转发数据
Fa0/23                   Root FWD 19      128.23    P2p      !端口状态为转发

VLAN0020
  Spanning tree enabled protocol rstp
           Root ID    Priority    20
           Address      0000.0C84.1692
           Cost         19
           Port         23(FastEthernet0/23)
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority    4116 (priority 4096 sys-id-ext 20)
           Address      00D0.FF65.029B
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 20

Interface                Role      Sts      Cost      Prio.Nbr Type
-----
```

```

Fa0/6          Desg FWD 19          128.6    P2p
Fa0/24          Altn BLK 19          128.24    P2p
Fa0/23          Root FWD 19          128.23    P2p
VLAN0020
Spanning tree enabled protocol rstp
Root ID Priority 20
Address 0000.0C84.1692
Cost 19
Port 23(FastEthernet0/23)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 4116 (priority 4096 sys-id-ext 20)
Address 00D0.FF65.029B
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 20

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/6	Desg	FWD	19	128.6	P2p
Fa0/24	Altn	BLK	19	128.24	P2p
Fa0/23	Root	FWD	19	128.23	P2p

从验证消息可以看到，在 VLAN 1、VLAN 10、VLAN 20 的生成树中，Switch-B 都为非根桥，意味着 3 个 VLAN 的流量都从 Switch-A 转发。从拓扑结构上可以看到，Switch-B 的 f0/24 端口为橙色，处于阻塞状态。

步骤 7：调整生成树状态，达到负载均衡。配置 Switch-B 为 VLAN 20 的根桥，VLAN 20 流量从 Switch-B 转发。

```

Switch-B>en
Switch-B#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-B(config)#spanning-tree vlan 20 root primary
!配置本地交换机为 vlan 20 的主根桥

```

步骤 8：验证调整状态后 Switch-B 上生成树的结果。

```

SWITCH-B#sh spanning-tree
..... !VLAN 1 部分没有配置，与前文相同，略去
VLAN0010
Spanning tree enabled protocol rstp
Root ID Priority 24586
Address 0000.0C84.1692
Cost 19
Port 23(FastEthernet0/23)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```



```

Bridge ID Priority    32778 (priority 32768 sys-id-ext 10)
Address      00D0.FF65.029B
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   20
    
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.1	P2p
Fa0/24	Altn	BLK	19	128.24	P2p
Fa0/23	Root	FWD	19	128.23	P2p

VLAN0020

Spanning tree enabled protocol rstp

```

Root ID    Priority    20
Address     00D0.FF65.029B
This bridge is the root          !本网桥为根桥
Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
    
```

```

Bridge ID Priority    20 (priority 0 sys-id-ext 20)
Address      00D0.FF65.029B
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   20
    
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/6	Desg	FWD	19	128.6	P2p
Fa0/24	Desg	FWD	19	128.24	P2p
Fa0/23	Desg	FWD	19	128.23	P2p

从显示信息可以看到，VLAN 20 的根桥已经转换为 Switch-B，VLAN 10 的根桥依然是 Switch-A。从拓扑结构上可以看到，Switch-B 被阻塞的 f0/24 端口已经转换为绿色，进入数据转发状态。

步骤 9：测试 PC 连通性，发现网络始终连通。

连接好后会发现两条链路中有一个端点显示为黄色标记，此标记表示该端口处于 block（关闭）状态。当前拓扑结构中仅有 Fa0/23 口互连的链路处在工作状态，而另一条 Fa0/24 口互连链路处于关闭状态，称为冗余链路，仅作为备份使用。



小贴士

此处也可在 Switch-A 上使用 “spanning-tree vlan 20 root secondary” 命令，使交换机 Switch-A 成为 VLAN 20 的次根桥（备份根桥）。

交换机在生成树选举中使用小的优先级作为根桥。可以使用 “spanning-tree vlan 20 priority 4096” 命令来直接改变交换机的优先级并参与选举。注意，因为 BID 的位格式决定了优先级必须为 4096 的整数倍，所以查看生成树状态时要在配置的优先级加上 VLAN ID。

相关知识

收敛是生成树过程的一个重要环节。收敛是指网络在一段时间内确定作为根桥的交换机、经过所有不同的端口状态，并且将所有交换机端口设置为其最终的生成树端口角色，而所有潜在的环路都被消除。收敛过程需要耗费一定时间，这是因为其使用不同的计时器来协调整个过程。

STP 收敛过程分为以下 3 个步骤。

步骤 1：选举根桥。根桥是所有生成树路径开销计算的基础，用于防止环路的各种端口角色也是基于根桥而分配的。

根桥选举在交换机完成启动时或者网络中检测到路径故障时触发。根桥选举是根据交换机的 BID 进行的，其中 BID=网桥优先级+VLAN ID，ID 最小者当选根桥。

步骤 2：选举根端口。

所有非根桥都产生一个根端口，即本网桥选择一个距根桥开销最小的端口作为根端口。

步骤 3：选举指定端口和非指定端口。当交换机确定了根端口后，还必须将剩余端口配置为指定端口（DP）或非指定端口（非 DP），以完成逻辑无环生成树。

交换网络中的每个网段只能有一个指定端口。当两个非根端口的交换机端口连接到同一个 LAN 网段时，会发生竞争端口角色的情况。这两台交换机会交换生成树消息，以确定哪个交换机端口是指定端口，哪个是非指定端口。

一般而言，交换机端口是否配置为指定端口由 BID 决定。但是，首要条件是具有到根桥的最低路径开销。只有当端口开销相等时，才考虑发送方的 BID。

STP 具有多种类型或变体。其中，某些变体是 Cisco 专有的，其他则是 IEEE 标准。

Cisco 专有的变体有：每个 VLAN 生成树协议（PVST）和增强型每个 VLAN 生成树协议（PVST+）；

IEEE 的生成树协议有多生成树（MSTP）和快速生成树（RSTP）。

学习小结

本任务介绍了交换机如何实现生成树协议，为互联网中提供了多条冗余备份链路，并解决互联网中的环路问题。默认情况下，两个交换机间的多条冗余链路仅有一条处于工作状态，其他链路都处于关闭状态，只有当其他链路出现故障或断开的情况下才会启用。但如果设置了生成树的 VLAN 负载均衡技术，则可以实现多条链路同时工作，这在一定程度上实现了网络带宽的扩容，从而提升了网络的速度。

任务 4 交换机的 DHCP 技术

在企业网络中，动态主机分配协议（Dynamic Host Configuration Protocol, DHCP）技术提供了有规划地分配 IP 地址，避免因用户私设 IP 地址而引起地址冲突。三层交换机提供了 DHCP 服务的功能，能够为用户动态分配 IP 地址，推送 DNS 服务地址等网络参数，使用户零配置上网。

学习情境

海成公司的员工反映经常出现 IP 地址冲突影响上网的情况，网络管理员决定在整个局域网上统一规划 IP 地址，用户使用动态获取地址方式接入局域网，既节约了地址空间，又避免



了地址冲突现象的发生。

情境分析

可提供 DHCP 服务的设备有路由器、三层交换机和专用的 DHCP 服务器。因为网络中使用的核心交换机、分布层交换机都为三层交换机，因此可以在分布层交换机上开启 DHCP 服务，配置用户地址池，统一分配规划的用户 IP 地址。

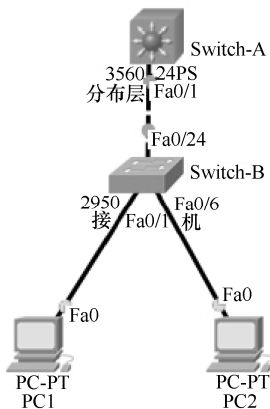


图 2-3-7 交换机 DHCP 功能配置拓扑图

所需设备：

- (1) Cisco Catalyst 3560 交换机 1 台。
- (2) Cisco Catalyst 2960 交换机 1 台。
- (3) PC 2 台。
- (4) 交 Console 线 1 条。
- (5) 直通线 2 条。
- (6) 交叉线 1 条。

任务拓扑结构如图 2-3-7 所示。

步骤实现

步骤 1：按照图 2-3-7 连接拓扑结构图。

步骤 2：配置交换机 A 的主机名称，并划分 VLAN

10 和 VLAN 20。

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-A
Switch-A(config)#vlan 10
Switch-A(config-vlan)#exit
Switch-A(config)#vlan 20
Switch-A(config-vlan)#exit
```

步骤 3：将交换机 A 的 fa0/1 端口配置为 Trunk。

```
Switch-A(config)#in f0/1
Switch-A(config-if)#sw mode trunk
Switch-A(config-if)#exit
```

步骤 4：开启交换机 A 的路由功能，并配置 VLAN 10 和 VLAN 20 的 IP 地址。

```
Switch-A(config)#ip routing
Switch-A(config)#int vlan 10
Switch-A(config-if)#ip add 192.168.10.1 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config-if)#int vlan 20
Switch-A(config-if)#ip add 192.168.20.1 255.255.255.0
Switch-A(config-if)#no shut
```

步骤 5：在三层交换机上配置 DHCP 服务。定义两个地址池，分别为 VLAN 10 和 VLAN 20 的 PC 分配地址。

```
Switch-A(config)#ip dhcp pool vlan10    !定义地址池，名称为 vlan10
Switch-A(dhcp-config)#network 192.168.10.0 255.255.255.0
!地址池的 IP 地址为 192.168.10.0/24 网段，子网掩码为 255.255.255.0
```

```

Switch-A(dhcp-config)#default-router 192.168.10.1 !默认网关为 192.168.10.1
Switch-A(dhcp-config)#dns-server 202.102.224.68 !推送 DNS 服务器地址
Switch-A(dhcp-config)#exit
Switch-A(config)#ip dhcp pool vlan20 !定义地址池名称为 vlan20
Switch-A(dhcp-config)#network 192.168.20.0 255.255.255.0
!地址也使用网段为 192.168.20.0/24
Switch-A(dhcp-config)#default-router 192.168.20.1
!默认网关为 192.168.20.1
Switch-A(dhcp-config)#dns-server 202.102.224.68 !推送 DNS 服务器地址
Switch-A(dhcp-config)#exit !返回全局配置
Switch-A(config)#service dhcp !开启 DHCP 服务

```

步骤 6: 在接入层交换机 Switch-B 上需要创建 VLAN 10、VLAN 20, 把 PC1 与 PC2 的端口分别加入到两个 VLAN 中。

```

Switch(config)#host Switch-B
Switch-B(config)#vlan 10
Switch-B(config-vlan)#vlan 20
Switch-B(config-vlan)#exit
Switch-B(config)#in f0/1
Switch-B(config-if)#sw acc vlan 10
Switch-B(config-if)#in f0/6
Switch-B(config-if)#sw acc vlan 20
Switch-B(config-if)#exit
Switch-B(config)#exit
Switch-B(config)#in f0/24
Switch-B(config-if)#sw mode trunk

```

步骤 7: 测试 PC 获取地址。

打开 PC 的桌面管理窗口, 发现 PC 已经获取 IP 地址。也可以在“运行”窗口中使用 ipconfig 命令进行验证, 如图 2-3-8 所示。



图 2-3-8 PC 动态获取 IP 地址成功



小贴士

设置 DHCP 服务器排除的 IP 地址: 假设要在 192.168.10/24 网段中保留前 20 个 IP 地址留做备用, 在 192.168.20.0/24 网中段保留前 100 个 IP 地址留做备用, 则使用如下命令进行配置。



```
SW(config)#ip dhcp excluded-address 192.168.10.2 192.168.10.20
SW(config)#ip dhcp excluded-address 192.168.20.2 192.168.20.100
```

验证保留地址是否生效，如图 2-3-9 所示。

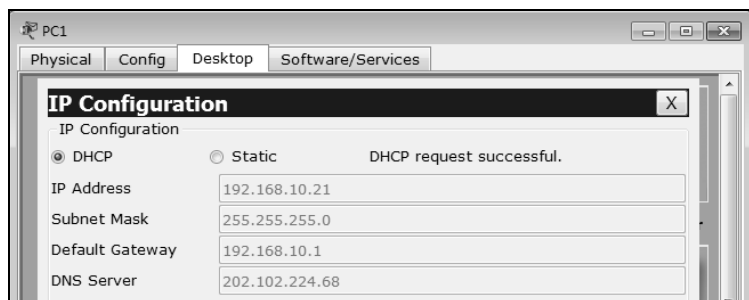


图 2-3-9 验证 DHCP 排除地址



小贴士

承载 DHCP 服务的下层协议是 UDP，占用的两个端口分别为 67、68。

相关知识

DHCP 为互联网上主机提供地址和配置参数。DHCP 基于 Client/Server 工作模式，DHCP 服务器需要为主机分配 IP 地址和提供主机配置参数。DHCP 具有以下功能。

- (1) 保证任何 IP 地址在同一时刻只能由一台 DHCP 客户机使用。
- (2) DHCP 应当可以给用户分配永久固定的 IP 地址。
- (3) DHCP 应当可以同用其他方法获得 IP 地址的主机共存（如手工配置 IP 地址的主机）。
- (4) DHCP 服务器应当向现有的 BOOTP（Bootstrap Protocol）客户端提供服务。

DHCP 有如下 3 种机制分配 IP 地址。

- (1) 自动分配（Automatic Allocation），DHCP 给客户端分配永久性的 IP 地址。
- (2) 动态分配（Dynamic Allocation），DHCP 给客户端分配一段时间后会过期的 IP 地址（或者客户端可以主动释放该地址）。
- (3) 手工配置（Manual Allocation），由网络管理员给客户端指定 IP 地址。网络管理员可以通过 DHCP 将指定的 IP 地址发给客户端。

3 种地址分配方式中，只有动态分配可以重复使用客户端不再需要的地址。

DHCP 消息的格式是基于 BOOTP 消息格式的，这就要求设备具有 BOOTP 中继代理的功能，并能够与 BOOTP 客户端和 DHCP 服务器实现交互。BOOTP 中继代理的功能，使得没有必要在每个物理网络中都部署一个 DHCP 服务器。

DHCP 请求 IP 地址的过程如下。

- (1) 主机发送 DHCPDISCOVER 广播包在网络中寻找 DHCP 服务器。
- (2) DHCP 服务器向本网络发送 DHCPOFFER 广播数据包，包含 IP 地址及地址租期等。
- (3) 主机发送 DHCPREQUEST 广播包，正式向服务器请求分配已提供的 IP 地址。
- (4) DHCP 服务器向主机发送 DHCPACK 单播包，确认主机的请求。

学习小结

本任务中使用三层交换机作为 DHCP 服务器，可以使下连的计算机通过交换机获取 IP 地址、子网掩码、网关和 DNS 服务器地址。当一个网络中计算机数量庞大时，使用 DHCP 服务，可以很方便地为每一台计算机配置好相应的 IP 参数，减轻了网络管理员分配 IP 地址的工作。

任务 5 交换机的 HSRP 技术

热备份路由器协议（Hot Standby Router Protocol HSRP）是一种容错协议，运行于局域网的多台路由器（或三层交换机）上，它将这几台路由器组织成一台“虚拟”路由器，其中一台路由器作为活动路由器（主设备），其余设备作为备份，并不断监控主设备，以便在主设备出现故障时，备份设备能够及时接管数据转发工作，为用户提供透明的切换，提高网络的可靠性。

学习情境

海成公司为了保证局域网络不间断运行，添加了一台备份核心交换机，以便在默认网关出现故障时接替网关工作，保障外网的畅通。

情境分析

如果系统中有多台路由器（三层交换机），则可以把它们组成一个“热备份组”，这个组形成了一个虚拟路由器。在任一时刻，一个组内只有一台路由器（三层交换机）是活动的，并由它来转发数据包，如果活动路由器发生了故障，将选择一个备份路由器来替代活动路由器，但是在本网络内的主机看来，虚拟路由器没有改变。所以主机仍然保持连接，没有受到故障的影响，这样就较好地解决了路由器切换问题。

添加两台三层交换机 3560，分别命名为 Switch-A 和 Switch-B，分别在 Switch-A 和 Switch-B 上配置 VLAN 10 和 VLAN 20 的网关，作为冗余备份；添加一台二层交换机 2960，作为接入交换机，命名为 Switch-C。在三台交换机上划分 2 个 VLAN：VLAN 10 和 VLAN 20，两台 PC 分别接入到两个 VLAN 中，网关采用虚拟网关。要求：VLAN 10 的网关在 Switch-A 上，VLAN 20 的网关在 Switch-B 上，出现故障时可以透明切换。

所需设备：

- (1) Cisco Catalyst 3560 交换机 2 台。
- (2) Cisco Catalyst 2960 交换机 1 台。
- (3) PC 2 台
- (4) Console 线 1 条。
- (5) 直通线 2 条。
- (6) 交叉线 3 条。

任务拓扑结构如图 2-3-10 所示。

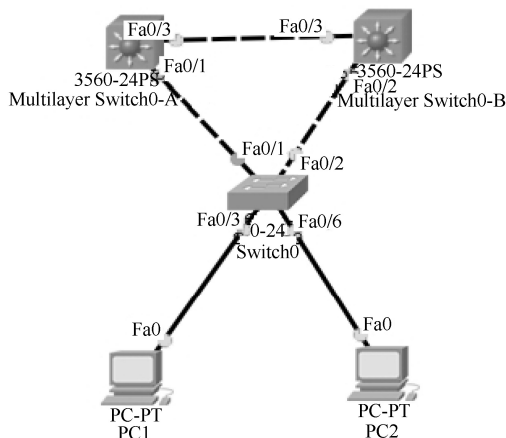


图 2-3-10 交换机 HSRP 配置拓扑图



网络参数设置如表 2-3-3 所示。

表 2-3-3 网络参数设置

设备名称	VLAN	IP 地址	网 关
Switch-A	VLAN 10, VLAN 20		192.168.10.1/24 192.168.20.1/24
Switch-B	VLAN 10, VLAN 20		192.168.10.2/24 192.168.20.2/24
Switch-C	VLAN 10, VLAN 20		
PC1	VLAN 10	192.168.10.10	192.168.10.39（虚拟）
PC2	VLAN 20	192.168.20.10	192.168.20.3（虚拟）

步骤实现

步骤 1：按照图 2-3-10 连接拓扑结构。

步骤 2：按照表 2-3-3 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置交换机 A 的主机名称，并划分 VLAN 10 和 VLAN 20。

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-A
Switch-A(config)#vlan 10
Switch-A(config-vlan)#exit
Switch-A(config)#vlan 20
Switch-A(config-vlan)#exit
```

步骤 4：将交换机 A 的 fa0/1 和 fa0/2 端口配置为 Trunk。

```
Switch-A(config)#in range f0/1-2
Switch-A(config-if)#sw mode trunk
Switch-A(config-if)#exit
```

步骤 5：开启交换机 A 的路由功能，并配置 VLAN 10 和 VLAN 20 的 IP 地址。

```
Switch-A(config)#ip routing      !开启路由功能
Switch-A(config)#in vlan 10
Switch-A(config-if)#ip add 192.168.10.1 255.255.255.0
Switch-A(config-if)#no shu
Switch-A(config-if)#in vlan 20
Switch-A(config-if)#ip add 192.168.20.1 255.255.255.0
Switch-A(config-if)#no shut
```

步骤 6：设置交换机 A 的 VTP 域为 abc，模式为服务器。

```
Switch-A(config)#vtp domain abc      !配置 VTP 域 abc
Switch-A(config)#vtp mode server      !配置 VTP 工作模式为服务器
```

步骤 7：配置交换机 B 的主机名称，并划分 VLAN 10 和 VLAN 20。

```
Switch>en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Switch-B
```

```
Switch-B(config)#vlan 10
Switch-B(config-vlan)#exit
Switch-B(config)#vlan 20
Switch-B(config-vlan)#exit
Switch-B(config)#
```

步骤 8: 将交换机 B 的 fa0/1 和 fa0/2 端口配置为 Trunk。

```
Switch-B(config)#in range f0/1-2
Switch-B(config-if)#sw mode trunk
Switch-B(config-if)#exit
```

步骤 9: 开启交换机 B 的路由功能, 并配置 VLAN 10 和 VLAN 20 的 IP 地址。

```
Switch-B(config)#ip routing      !开启路由功能
Switch-B(config)#in vlan 10
Switch-B(config-if)#ip add 192.168.10.2 255.255.255.0
Switch-B(config-if)#no shu
Switch-B(config-if)#in vlan 20
Switch-B(config-if)#ip add 192.168.20.2 255.255.255.0
Switch-B(config-if)#no shut
```

步骤 10: 设置交换机 B 的 VTP 域为 abc, 模式为客户端。

```
Switch-B(config)#vtp domain abc      !配置 VTP 域 abc
Switch-B(config)#vtp mode client      !配置 VTP 工作模式为客户端
```

步骤 11: 配置交换机 C 的主机名称、Trunk 链路、VTP 域为 abc、模式为客户端, 并将端口 fa0/3 加入 VLAN 10、fa0/6 加入 VLAN 20。

```
Switch>en
Switch#conf t
Switch(config)#hostname Switch-C
Switch-C(config)#in range f0/1-2
Switch-C(config-if)#sw mode trunk
Switch-C(config)#vtp domain abc      !配置 VTP 域 abc
Switch-C(config)#vtp mode client      !配置 VTP 工作模式为客户端
Switch-C(config)#int f0/3
Switch-C(config-if)#switchport access vlan10
Switch-C(config-if)#int f0/6
Switch-C(config-if)#switchport access vlan20
```

步骤 12: 配置 Switch-A 的 HSRP 冗余网关组。

```
Switch-A(config)# in vlan 10
Switch-A(config-if)#standby 10 priority 110
!将接口加入 standby 10 组中, 优先级为 110
Switch-A(config-if)#standby 10 ip 192.168.10.3 !设置 standby 10 组的虚拟 IP 地址
Switch-A(config-if)#standby 10 preempt          !允许 standby 10 组的抢占功能
Switch-A(config-if)#standby 10 track fa 0/1      !设置 standby 10 组监控 fa0/1 接口
Switch-A(config-if)#exit
Switch-A(config)#in vlan 20                      !进入接口 vlan 20
Switch-A(config-if)#standby 20 priority 100
!接口加入 standby 20 虚拟组, 优先级为 100
```



```
Switch-A(config-if)#standby 20 ip 192.168.20.3 !standby 20 组的虚拟 IP 地址
```

步骤 13: 配置 Switch-B 的 HSRP 冗余网关组。

```
Switch-B(config)# in vlan 10
```

```
Switch-B(config-if)#standby 10
```

!将接口加入 standby 10 组中, 优先级为默认值 100

```
Switch-B(config-if)#standby 10 ip 192.168.10.3 !设置 standby 10 组的虚拟 IP 地址
```

```
Switch-B(config-if)#exit
```

```
Switch-B(config)#in vlan 20 !进入接口 vlan20
```

```
Switch-B(config-if)#standby 20 priority 110
```

!将接口加入 standby 20 虚拟组, 优先级为 100

```
Switch-B(config-if)#standby 20 ip 192.168.20.3 !standby 20 组的虚拟 IP 地址
```

```
Switch-B(config-if)#standby 20 preempt !允许 standby 20 组的抢占功能
```

```
Switch-B(config-if)#standby 20 track fa 0/2 !设置 standby 20 组监控 f0/2 接口
```

步骤 14: 验证 PC 的连通性, 验证虚拟网关是否可用, 如图 2-3-11 所示。

```
PC>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Reply from 192.168.20.10: bytes=32 time=0ms TTL=127
Reply from 192.168.20.10: bytes=32 time=1ms TTL=127
Reply from 192.168.20.10: bytes=32 time=11ms TTL=127
Reply from 192.168.20.10: bytes=32 time=0ms TTL=127

Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 3ms

PC>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=6ms TTL=128
Reply from 192.168.10.10: bytes=32 time=11ms TTL=128
Reply from 192.168.10.10: bytes=32 time=4ms TTL=128
Reply from 192.168.10.10: bytes=32 time=6ms TTL=128
```

图 2-3-11 验证虚拟网关的可用性

步骤 15: 在交换机 Switch-A 上使用 show standby 命令, 查看当前 standby 工作状态。

```
Switch-A#show standby
```

```
Vlan10 - Group 10 (version 2) !vlan 10 组
```

```
State is Active !本地状态为活动状态(主设备)
```

```
5 state changes, last state change 00:49:45
```

```
Virtual IP address is 192.168.10.3 !虚拟 IP 地址
```

```
Active virtual MAC address is 0000.0C9F.F00A
```

```
Local virtual MAC address is 0000.0C9F.F00A (v2 default)
```

```
Hello time 3 sec, hold time 10 sec
```

```
Next hello sent in 0.679 secs
```

```
Preemption disabled
```

```
Active router is local
```

```

Standby router is 192.168.10.2, priority 120 (expires in 7 sec)
!备份网关的地址和优先级

Priority 100 (configured 120)
Group name is hsrp-Vl1-10 (default)          !此 HSRP 组的默认组名
Vlan20 - Group 20 (version 2)                !HSRP 组 20 (HSRP 版本号为 2)
State is Standby                             !本地设备的 HSRP 状态为 standby (备份)

  6 state changes, last state change 00:49:55
Virtual IP address is 192.168.20.3           !standby 20 组的虚拟 IP 地址
Active virtual MAC address is 0000.0C9F.F014
Local virtual MAC address is 0000.0C9F.F014 (v2 default)
Hello time 3 sec, hold time 10 sec
!HSRP 的 hello 计时器和抑制计时器, 下轮 hello 时间

Next hello sent in 1.188 secs
Preemption disabled
Active router is 192.168.20.2, priority 100 (expires in 7 sec)
!活动路由器的 IP 地址为 192.168.20.2, 本地优先级为 100, 7s 后将到期

MAC address is 0000.0C9F.F014
Standby router is local                       !本地路由器为备份路由器 (standby)
Priority 100 (default 100)                   !优先级为默认值 100
Group name is hsrp-Vl2-20 (default)

Switch-A#

```

此时 Switch-A 反馈信息显示, VLAN 10 组的主设备是 Switch-A, VLAN 20 的主设备是 Switch-B。

步骤 16: 拔掉交换机 Switch-C 的 fa0/2 接口的上连线, 再次验证 PC 的连通性, 发现此时有短暂的丢包现象发生以后, 又恢复了连通, 如图 2-3-12 所示。

```

PC>ping 192.168.20.10

Pinging 192.168.20.10 with 32 bytes of data:

Request timed out.
Request timed out.
Reply from 192.168.20.10: bytes=32 time=0ms TTL=127
Reply from 192.168.20.10: bytes=32 time=0ms TTL=127

```

图 2-3-12 验证 HSRP



小贴士

管理员可以使用一系列 show standby 命令来检查 HSRP 的状态, 其中有多参数可供使用。例如, 命令 show standby brief 可以简单显示 HSRP 的汇总配置。管理员可以确认每个备用组中的本地路由器邻居。

相关知识

HSRP 是思科平台上的一种特有技术, 是思科公司的私有协议。

该协议中含有多台路由器, 对应一个 HSRP 组。该组中只有一台路由器承担转发用户流



量的职责，这就是活动路由器。当活动路由器失效后，备份路由器将承担该职责，成为新的活动路由器。这就是热备份的原理。

为了减少网络的数据流量，在设置完活动路由器和备份路由器之后，只有活动路由器和备份路由器定时发送 HSRP 报文。如果活动路由器失效，则备份路由器将接管成为活动路由器。如果备份路由器失效或者变为活动路由器，则将其他路由器被选为备份路由器。

在实际的一个特定的局域网中，可能有多个热备份组并存或重叠。每个热备份组模仿一台虚拟路由器工作，它有一个公共的 MAC 地址和 IP 地址。该 IP 地址、组内路由器的接口地址、主机在同一个子网内，但是不能一样。当在一个局域网上有多个热备份组存在时，把主机分布到不同的热备份组中，可以使负载得到分担。

学习小结

本任务介绍了思科的 HSRP 技术，它和 IEEE 的 VRRP 技术都是网关设备的冗余技术，在现代企业网络中应用广泛，一般和 PVST（每个 VLAN 生成树）或者多生成树协议结合，部署双核心的网络架构，极大程度地增加了网络的可靠性，实现了负载均衡，提高了网络的效率。

项目考核

某公司正在升级局域网，在保护已有的网络架构的基础上，新添加了一台核心交换机 Cisco Catalyst 3560 作为备份网关，并增加了相应的冗余链路接入 Internet，整个网络的拓扑结构如图 2-3-13 所示，请根据表 2-3-4 对交换机做相应配置。

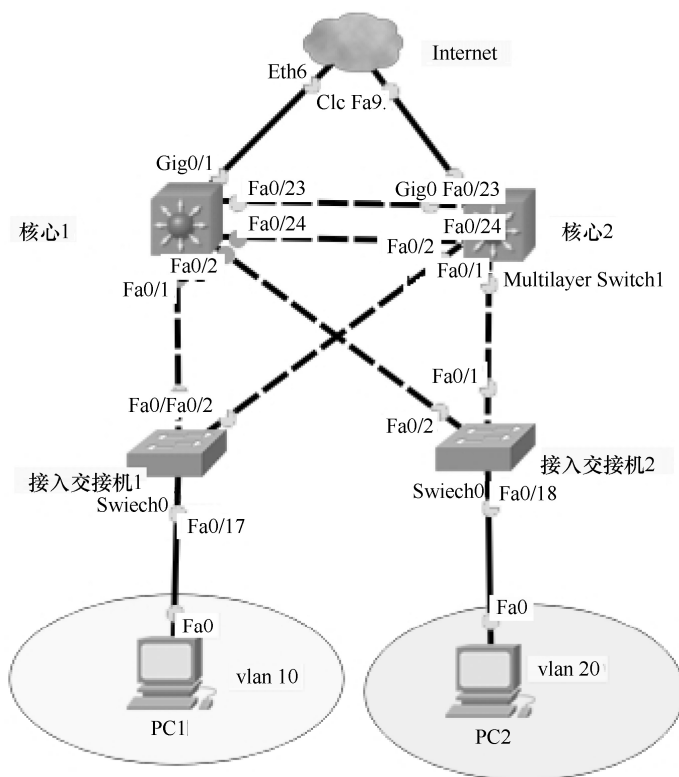


图 2-3-13 某公司拓扑结构图

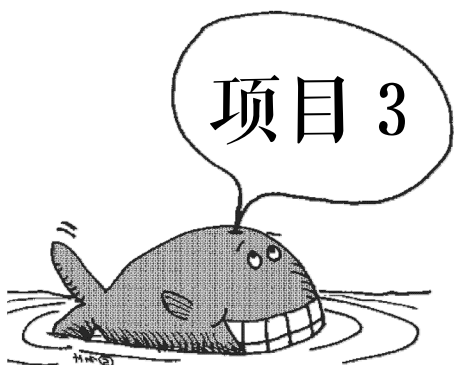
交换机参数配置如表 2-3-4 所示。

表 2-3-4 交换机参数配置

交 换 机	VLAN	IP 地址	HSRP 组	虚拟网关地址
核心 1	VLAN 10	172.16.10.252/24	10	172.16.10.254/24
	VLAN 20	172.16.20.252/24	20	172.16.20.254/24
核心 2	VLAN 10	172.16.10.253/24	10	172.16.10.254/24
	VLAN 20	172.16.20.253/24	20	172.16.20.254/24

配置要求：

- （1）按照拓扑结构图，选择合适线缆连接网络设备与 PC，设置 PC 动态获取 IP 地址及网关。
- （2）在接入交换机上划分相应的 VLAN，并将 PC 添加到 VLAN 中。
- （3）在核心交换机上配置交换机之间的链路聚合、VLAN 的网关，开启 DHCP 服务，实现 VLAN 之间的互访。
- （4）在核心交换机上使用 PVST 技术和 HSRP 技术做网关冗余和负载均衡，使 PC1 的数据由核心 1 转发，核心 1 故障时由核心 2 转发；PC2 的数据由核心 2 转发，核心 2 故障时由核心 1 转发。
- （5）监控核心交换机上连接口和下连接口，如发生故障，则立即切换网关设备。



路由技术基础

项目学习说明

路由器是连接互联网中各局域网和广域网的不可缺少的网络设备，它会根据整个网络的通信情况自动进行路由选择，以最佳的路径，按先后顺序发送信息给其他网络设备，从而实现信息的路由转发。目前路由器已经广泛应用于各行各业，不同档次的产品已经成为实现各种骨干网内部连接、骨干网间互连和骨干网与互联网互连互通业务的主力军。

本项目重点学习路由器的设置、路由器的基本配置、单臂路由的配置、路由器的 DHCP 配置和路由器的 Telnet 配置。

学习能力目标

- 实训 1：路由器的设置。
- 实训 2：路由器的基本配置。
- 实训 3：单臂路由的配置。
- 实训 4：路由器系统的备份与恢复。
- 实训 5：路由器的 DHCP 配置。
- 实训 6：路由器的 Telnet 配置。

职业能力目标

- 能完成模拟器中路由器的设置。
- 能熟练使用路由器的基本配置命令。
- 能实现路由器的单臂路由的配置。
- 能实现路由器的 DHCP 的配置。
- 能实现路由器的 TELNET 的配置。
- 能实现路由器的 SSH 的配置。

实训 1 路由器的设置

路由器一般提供了许多模块化功能，通过对模块的添加、更换，以支持不断提高的网络带宽和服务质量要求。路由器添加模块就像为计算机添加一张网卡一样，可以增加网络的接口。一个路由器，模块越多，功能就越多，价格也相对较高。

学习情境

海成公司因为业务的扩大，购买了新的路由器，网络管理员对此并不太熟悉，因此在 Cisco Packet Tracer 中先练习如何使用。Cisco Packet Tracer 提供了多款路由器供用户进行选择，还为路由器提供了大量的可选模块，提供了很好的环境。

情境分析

默认情况下，在 Cisco Packet Tracer 6.1 Instructor 中添加的路由器没有广域网模块，不能进行 DCE 串口线的连接，因此在完成本实训时首先要为路由器添加相关的功能性模块。

下面以型号为 2911 的路由器来学习和掌握 Cisco Packet Tracer 6.1 Instructor 模拟器中路由器的一些设置方法，拓扑结构如图 3-1-1 所示，按照表 3-1-1 和表 3-1-2 添加相应设备、更改标签名称并连接设备。

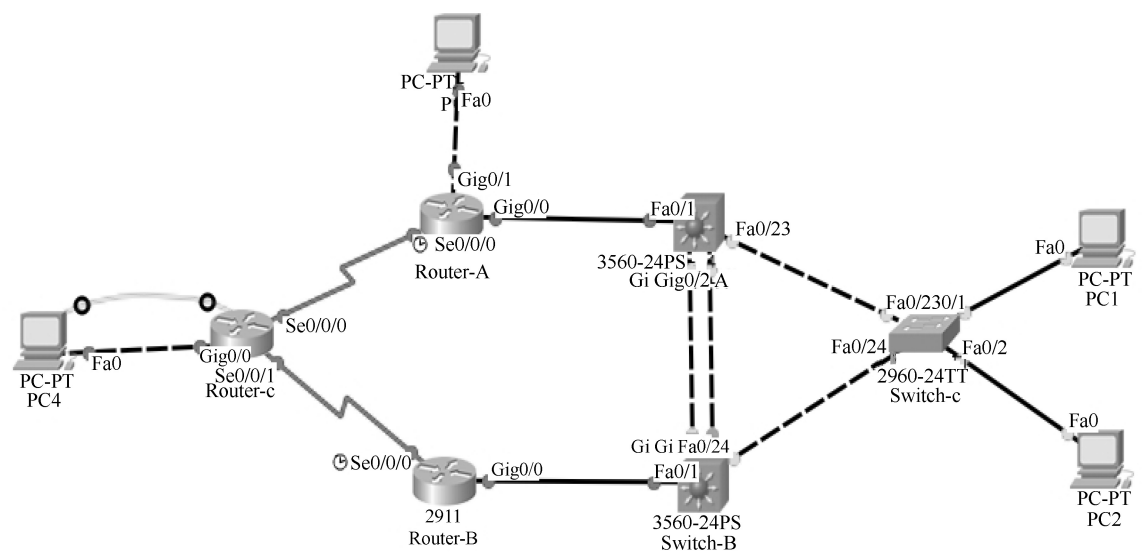


图 3-1-1 海成公司网络拓扑图

表 3-1-1 网络设备与标签名称

设备类型	数量/台	标签名称
2911 路由器	3	Router-A、Router-B、Router-C
3560-24 三层交换机	2	Switch-A、Switch-B
2960 二层交换机	1	Switch-C
PC	4	PC1、PC2、PC3、PC4



表 3-1-2 网络设备的相应端口

设备名称及端口	对端设备名称及端口	线 缆 类 型
Router-A: S0/0/0	Router-C: S0/0/0	DCE 串口线
Router-A: Gi0/0	Switch-A: fa0/1	直通线
Router-B: S0/0/0	Router-C: S0/0/1	DCE 串口线
Router-B: gi0/0	Switch-B: fa0/1	直通线
Router-C: Console	PC4: RS-232	配置线
Switch-A: Gi0/1、Gi0/2	Switch-B: Gi0/1、Gi0/2	交叉线
Switch-A: fa0/23	Switch-C: fa0/23	交叉线
Switch-B: fa0/24	Switch-C: fa0/24	交叉线
PC1	Switch-C: fa0/1	直通线
PC2	Switch-C: fa0/2	直通线
PC3	Router-A: Gi0/1	交叉线
PC4	Router-C: Gi0/0	交叉线

步骤实现

步骤 1：根据图 3-1-1 所示的拓扑结构添加网络设备。在 Cisco Packet Tracer 6.1 Instructor 的工作区中添加 3 台 2911 路由器、2 台 3560 三层交换机、1 台 2960 二层交换机和 4 台 PC，并调整相应位置，如图 3-1-2 所示。

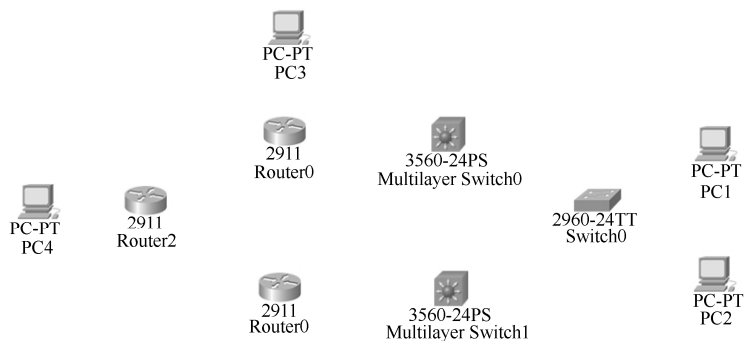


图 3-1-2 添加的网络设备

步骤 2：更改各设备的标签名称，以 Router0 为例。在 Router0 上单击，在打开的窗口中选择“Config”选项，在“显示名称”文本框中输入“Router-A”，关系“Router-A”对话框，如图 3-1-3 所示。



图 3-1-3 修改显示名称

步骤 3：使用同样的方法为其他设备（包括 PC）更改显示名称，如图 3-1-4 所示。

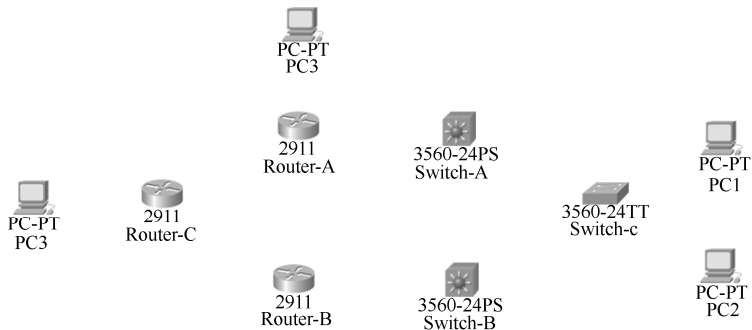


图 3-1-4 修改后的所有设备显示名称

步骤 4：在实际操作中，为路由器添加模块时需要在断电的情况下添加，否则会损坏设备。默认情况下，Cisco Packet Tracer 6.1 Instructor 中路由器的电源是打开的，因此在添加模块前首先要关闭路由器的电源，如图 3-1-5 所示。

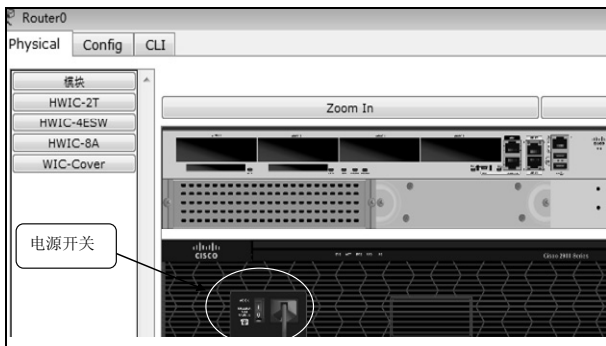


图 3-1-5 关闭路由器的电源

步骤 5：在模块区域中找到所需要的模块，选中该模块，将其拖动到模块的添加区域。添加模块时要注意模块的形状及大小，选择正确的插槽。图 3-1-6 所示即为路由器 Router-A 添加一个 HWIC-2T 串口模块。

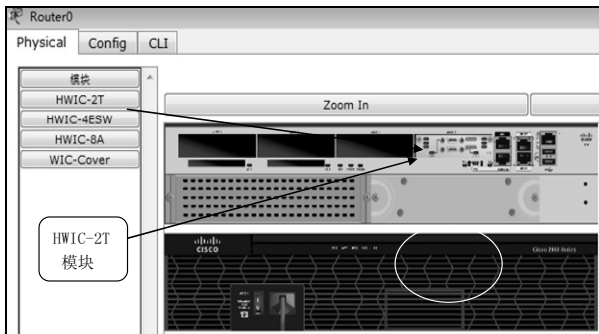


图 3-1-6 添加 HWIC-2T 模块

步骤 6：使用同样的方法为路由器 Router-B 和 Router-C 添加 HWIC-2T 模块。



步骤 7：查看路由器的端口。将鼠标指针放置在工作区路由器图标上停留一会儿，会显示一个黄色底纹的提示信息框，如图 3-1-7 所示，可以查看到端口类型、IP 地址等信息。

端口	线路	VLAN	IP地址	IPv6地址	MAC地址
GigabitEthernet0/0	Down	--	<not set>	<not set>	000C.852C.8B01
GigabitEthernet0/1	Down	--	<not set>	<not set>	000C.852C.8B02
GigabitEthernet0/2	Down	--	<not set>	<not set>	000C.852C.8B03
Serial0/0/0	Down	--	<not set>	<not set>	<not set>
Serial0/0/1	Down	--	<not set>	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	0060.5C6C.D1DE
主机名称:Router-C					
物理位置:城际, 城市家园, 公司办公室, 主要的工作棚, 机架					

图 3-1-7 查看路由器端口

步骤 8：路由器与计算机的互连通常是通过路由器的局域网接口与计算机的网卡接口进行的，如图 3-1-8 所示。



小贴士

路由器本身就是一台没有显示器的计算机主机，在计算机与路由器直接互联时，应采用交叉线进行互联，而不能使用直通线。虽然现在市面上也存在有使用直通线互联的路由器，但在 Cisco Packet Tracer 软件中是不支持的。

步骤 9：路由器与交换机的互连通常是通过路由器的局域网接口与交换机接口进行的，如图 3-1-9 所示。

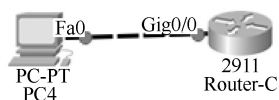


图 3-1-8 路由器与计算机互连

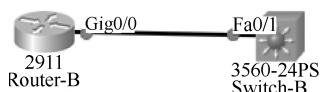


图 3-1-9 路由器与交换机互连



小贴士

从前面所有的拓扑图中会发现一个共同点，即所有已连接的端口的状态标记都是红色的，这是因为当前路由器还没有进行配置，所有端口都处于 Shutdown（关闭）状态。

步骤 10：通过上面的学习，请读者使用正确的线缆完成本实训的所有网络设备的连接，最终效果应与图 3-1-1 一致。

相关知识

路由器具有非常强大的网络连接和路由功能，它可以与各种各样的网络进行物理连接，这就决定了路由器的接口技术非常复杂，越是高档的路由器，其接口种类也就越多，因为它所能连接的网络类型非常多。路由器的端口主要分为局域网端口、广域网端口和配置端口三大类。

路由器与路由器互连的方式有很多，因为路由可添加的模块很多，造成路由器端口类型很多，而不同端口类型使用不同的线缆进行互连。其主要分为以下 3 种。

（1）路由器通过广域网串口互连，要使用专用的 DTE 和 DCE 串口线连接。

（2）路由器通过局域网以太网口互连，一般使用双绞线进行互连，且一定要使用交叉线进行连接，用直通线连接是无法通信的。

（3）路由器的调整网络接入，通常使用光纤接入。

在实现的网络过程中，需要对网络设备添加或卸下模块时，一定要先断电，才可以

操作。

学习小结

本实训讲述了路由器模块添加的方法，路由器各种端口使用的线缆类型和路由器端口的标签名称的更改，由于真实设备中添加模块和模拟器是有区别的，所以有条件时，最好在真实设备上练习，掌握操作方法熟练。

实训 2 路由器的基本配置

路由器在网络中担任了非常重要的角色，因此路由器的基本配置显得尤为重要。路由器的基本配置有：给设备命名、登录信息、设置接口的 IP 地址、设置特权密码和端口配置等。

学习情境

海成公司因业务发展需求，需要购买一台路由器扩展现有网络，根据公司的网络拓扑规划，网络管理员将刚买回来的新路由器经过配置后投入使用。

情境分析

网络管理员拿到刚买的路由器时，首先要对出厂的路由器进行配置，可以通过路由器的 Console 口进行配置。路由器上有一个 Console 口，从交换机端口标识中可以识别到，之后通过出厂自带的配置线进行连接即可进行配置。

所需准备：

- (1) Cisco2911 路由器 1 台。
- (2) PC 1 台。
- (3) 交叉线 1 条。
- (4) Console 线 1 条

实训拓扑结构如图 3-2-1 所示。



图 3-2-1 路由器基本配置拓扑图

步骤实现

步骤 1：按照图 3-2-1 选择并连接设备。单击 PC，在弹出的窗口中选择“Desktop”选项卡，进入如图 3-2-2 所示的界面，选择“Terminal”选项，弹出“终端配置”对话框。

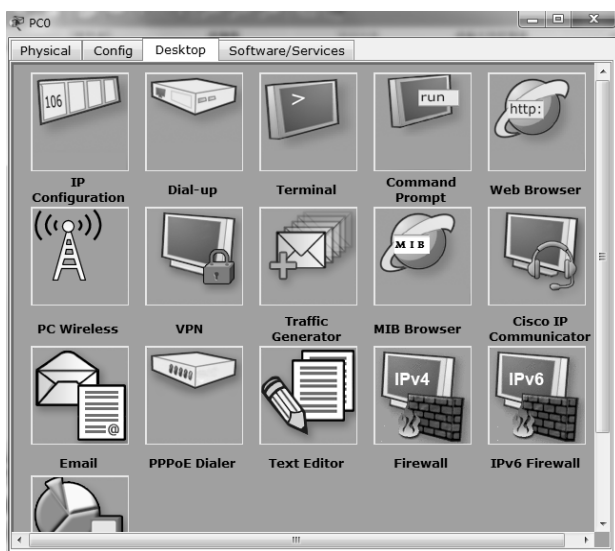


图 3-2-2 PC 桌面应用程序



步骤 2：调整超级终端的参数，如图 3-2-3 所示，单击“确定”按钮。



图 3-2-3 “终端配置”对话框

步骤 3：给路由器加电，超级终端显示路由器的自检信息，自检结束后出现如下命令提示。

```
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2911/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image :
#####
## [OK]
Smart Init is enabled
smart init is sizing iomem
TYPE MEMORY_REQ
Onboard devices &
buffer pools 0x022F6000
-----
TOTAL: 0x022F6000
Rounded IOMEM up to: 36Mb.
Using 6 percent iomem. [36Mb/512Mb]
Cisco CISCO2911/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
3 Gigabit Ethernet interfaces
```

```

DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

```

```

--- System Configuration Dialog ---

```

```

Continue with configuration dialog? [yes/no]:

```

步骤 4：路由器与交换机一样，都有相应的配置模式，而且切换的方法也相同。但不同的是，路由器在第一次进行配置时有配置向导，如图 3-2-4 所示。通过此配置向导，可以进行一些简单的基本配置，但作为专业的网络管理员，通常不采用此方式。因此，可以退出配置向导，输入“NO”即可进入正常配置方式。

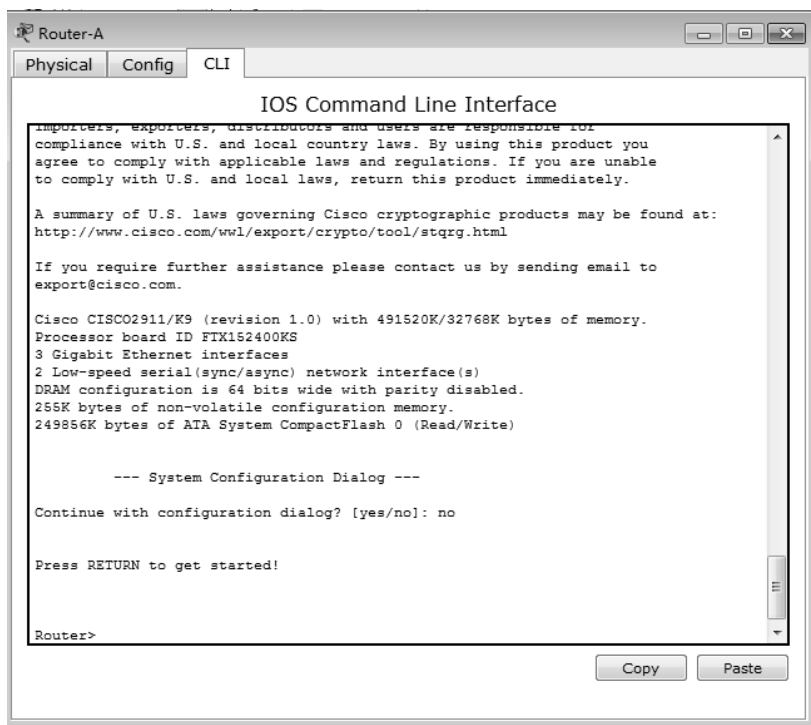


图 3-2-4 路由器配置向导界面

步骤 5：思科公司的路由器出厂时没有定义密码，用户按 Enter 键即可直接进入普通用户模式，可以使用权限允许范围内的命令，需要帮助时可以随时输入“？”，输入 enable 命令，按 Enter 键即可进入超级配置模式，在超级配置模式下，用户拥有最大的权限，可以任意配置，需要帮助时可以随时输入“？”。

```

Router>?
Exec commands:
<1-99> Session number to resume
connect Open a terminal connection
disable Turn off privileged commands
disconnect Disconnect an existing network connection

```



```
enable Turn on privileged commands
exit Exit from the EXEC
logout Exit from the EXEC
ping Send echo messages
resume Resume an active network connection
show Show running system information
ssh Open a secure shell client connection
telnet Open a telnet connection
terminal Set terminal line parameters
traceroute Trace route to destination
Router>
```

步骤 6：路由器的配置模式切换。

Router>	! 进入用户模式
Router>enable	! 进入特权模式
Router#configure terminal	! 进入全局配置模式
Router(config)#int gi0/0	! 进入端口配置模式
Router(config-if)#exit	! 返回上一级
Router(config)#end	! 直接返回特权模式
Router#write	! 保存配置
Router#	

步骤 7：为路由器命名。

Router#config t	! 进入全局配置模式
Router(config)#hostname Router-A	! 将路由器命名为 Router-A
Router-A(config)#	

步骤 8：为路由器设置时间。

```
Router-A#
Router-A#clock set 17:05:00 23 nov 2014
Router-A#show clock
*17:5:5.882 UTC Sun Nov 23 2014
Router-A#
```

步骤 9：为路由器设置特权密码。

```
Router-A#
Router-A#conf t
Router-A(config)#enable password 123456
Router-A(config)#enable secret 654321
```

步骤 10：为路由器设置 Console 密码。

```
Router-A#
Router-A#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router-A(config)#line console 0
Router-A(config-line)#password 123
Router-A(config-line)#login
Router-A(config-line)#]
```

步骤 11：为路由器设置 Telnet 登录密码。

```
Router-A#
Router-A#config t
Router-A(config)#line vty 0 5
Router-A(config-line)#password 321
Router-A(config-line)#login
Router-A(config-line)#
```

步骤 12：将所有明文密码变为密文显示。

```
Router-A#
Router-A#conf t
Router-A(config)#service password-encryption
Router-A(config)#
```

步骤 13：配置标语。

```
Router-A#
Router-A#conf t
Router-A(config)#banner motd $ Authorized Access Only!$
Router-A(config)#
```



小贴士

- (1) 超级终端中的配置是对路由器的操作，这时的 PC 只是输入输出设备。
- (2) 要按照 (9600, 8, 无, 1, 无) 设置终端的硬件参数，否则计算机将无法配置路由器。
- (3) 要选择正确的计算机 COM 口。

相关知识

1. 路由器的管理方式

路由器的管理方式可以分为带外管理和带内管理。带内管理，是指网络的管理控制信息与用户网络的承载业务信息通过同一个逻辑信道传送，简而言之，就是占用业务带宽。带外管理，是指网络的管理控制信息与用户网络的承载业务信息在不同的逻辑信道传送，即设备提供了专门用于管理的带宽。目前很多高端的交换机都带有带外网管接口，使网络管理的带宽和业务带宽完全隔离，互不影响，构成单独的网管网。通过 Consloe 口管理是最常用的带外管理方式，通常用户会在首次配置交换机或者无法进行带内管理时使用带外管理方式。带外管理方式也是使用频率最高的管理方式。使用带外管理的时候，可以采用 Windows 操作系统自带的超级终端程序来连接交换机，当然，用户也可以使用自己熟悉的终端程序。带外管理方式就是通过路由器的 Consloe 口管理路由器的方式，不占用路由器的网络接口，特点是线缆特殊，需要近距离配置。第一次使用路由器时，必须采用 Console 口对路由器进行配置，使其支持 Telnet 管理。带内管理的方式有 Telnet 和 Web。

2. 路由器的命令行操作模式

路由器的命令行操作模式主要有：用户模式、特权模式、配置模式。

用户模式：进入路由器后的第一个操作模式，此模式下用户只具有最底层的权限，可以查看路由器的软、硬件版本信息，但不能对路由器进行配置。

特权模式：用户模式的下一级模式，在此模式下用户可以对路由器的配置文件进行管理，查看路由器的配置信息，进行网络的测试和调试等。

全局配置模式：特权模式的下一级模式，在此模式下可以配置路由器的全局参数，如主机名、登录信息等，在此模式下可以进入下一级的配置模式，对路由器的具体功能进行配置。



课堂训练

教师演示完以上步骤后，让每个学生根据步骤进行操作，并对其进行验证，将验证后的结果截图并保存，学生操作完成后，教师对其结果进行检查。

知识拓展

1. 热键和快捷方式

IOS CLI 提供热键和快捷方式，以便配置、监控和排除故障。

向下箭头：用于在前面使用过的命令列表中向前滚动。

向上箭头：用于在前面使用过的命令列表中向后滚动。

Tab：完成只键入了一部分的命令或关键字的其余部分。

Ctrl-A：移至行首。

Ctrl-E：移至行尾。

Ctrl-R：重新显示一行。

Ctrl-Z：退出配置模式并返回用户模式。

Ctrl-C：退出配置模式或放弃当前的命令。

Ctrl-Shift-6：用于中断诸如 ping 或 traceroute 之类的 IOS 进程。

部分快捷方式的详细说明如下。

Tab：如果输入的缩写命令或缩写参数包含足够多的字母，已经可以和当前可用的任意其他命令或参数区分开，则可使用 Tab 填写该缩写命令或缩写参数剩余的部分。当已输入足够多的字符，可以唯一确定命令或关键字时，可按 Tab 键，CLI 即会显示该命令或参数剩余的部分。此技巧在学习过程中很有用，因为它可以使用户看到命令或关键字的完整词语。

Ctrl-R：重新显示行会刷新刚键入的行。使用 Ctrl-R 可重新显示命令行。例如，IOS 可能会在用户键入命令行的过程中向 CLI 返回一条消息。用户可使用 Ctrl-R 刷新该行，这样无需重新键入该行。

在此例中，在用户输入命令的过程中返回了一条与接口故障相关的消息。

```
Switch# show mac-
16w4d: %LINK-5-CHANGED: Interface FastEthernet0/10, changed state to down
16w4d: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10,
changed state to down
```

要重新显示用户刚才正在键入的行，则使用 Ctrl-R，即

```
Switch# show mac
```

Ctrl-Z：退出配置模式将离开所有配置模式并返回特权模式。因为 IOS 具有分层模式结构，有时可能发现自己处于下层的层次中，要想返回处于顶层的特权模式，则无需逐级退出，只要使用 Ctrl-Z 即可直接返回。

向上和向下箭头：上述命令键将调用输入过的命令历史。Cisco IOS 将用户之前键入的几个命令和字符保存在缓冲区中，以供用户重新调用。缓冲区消除了重复键入命令的必要。

用户可使用特定的按键序列以在这些保存在缓冲区中的命令之间滚动。向上箭头键（Ctrl-P）用于显示输入过的前一个命令。每次按此键时，将依次显示较早输入的一条命令。向下箭头键（Ctrl-N）用于依次显示命令历史记录中较晚输入的一条命令。

Ctrl-Shift-6：Escape 序列会中断所有正在运行的进程。当从 CLI 启动一个 IOS 进程（如 ping 或 traceroute）后，该命令会运行到完成或被中断为止。当该进程正在运行时，CLI 无响应。要中断输入并与 CLI 交互，可按 Ctrl-Shift-6。

Ctrl-C：用于中断命令输入并退出配置模式。这在输入需要撤销的命令时很有用。

缩写命令或缩写参数：命令和关键字可缩写为可唯一确定该命令或关键字的最短字符数。例如，configure 命令可缩写为 conf，因为 configure 是唯一一个以 conf 开头的命令，不能缩写为 con，因为以 con 开头的命令不只一个。

关键字也可缩写，例如，Switch# show interfaces 可以缩写为 Switch# show int 或 Switch# sh int。

学习小结

本实训重点介绍了路由器的基本设置，基础知识的掌握很重要，读者要多练习，加以熟练，否则后面使用的时候很难得心应手。

实训 3 单臂路由的配置

学习情境

海成公司的管理员对部门划分了 VLAN 后，发现两个部门之间无法通信，但有时两个部门的员工需要进行通信，管理员现要通过简单的方法来实现此功能。

情境分析

通过在交换机上划分适当数目的 VLAN，不仅能有效隔离广播风暴，还能提高安全性及网络带宽的利用效率。划分 VLAN 之后，VLAN 与 VLAN 之间是不能通信的，使用路由器的单臂路由功能可以解决这个问题。

所需准备：

- (1) Cisco 2911 路由器 1 台。
- (2) Cisco Catalyst 2960 交换机 1 台。
- (3) PC 2 台。
- (4) 直通双绞线 3 条。
- (5) Console 线 1 条。

实训拓扑结构如图 3-3-1 所示。

网络参数设置如表 3-3-1 所示。

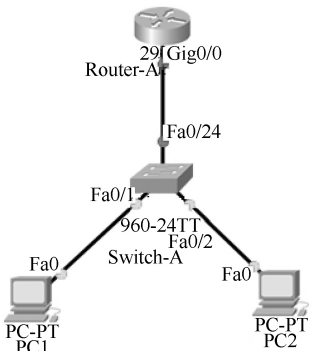


图 3-3-1 单臂路由配置拓扑

表 3-3-1 网络参数设置

设备	端口	IP 地址	子网掩码	网关
Router-A	G0/0	无	无	无
Switch-A	Fa0/1	VLAN 10		
	Fa0/2	VLAN 20		
	Fa0/24	无	无	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1

步骤实现

步骤 1：按照图 3-3-1 连接网络拓扑结构。



步骤 2：按照表 3-3-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：在交换机 A 上配置主机名。

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#host Switch-A
Switch(config)#
```

步骤 4：在交换机 A 上创建 VLAN 10，端口成员为 fa0/1；创建 VLAN 20，端口成员 2。

```
Switch-A(config)#vlan 10
Switch-A(config-vlan)#vlan 20
Switch-A(config-vlan)#exit
Switch-A(config)#int fa0/1
Switch-A(config-if)#switchport access vlan 10
Switch-A(config-if)#int fa0/2
Switch-A(config-if)#switchport access vlan 20
Switch-A(config-if)#
```

步骤 5：在交换机 A 上配置 Trunk。

```
Switch-A(config-if)#int fa0/24
Switch-A(config-if)#switchport mode trunk
Switch-A(config-if)#
```

步骤 6：路由器 A 的配置。

```
Router>enable
Router#conf t
Router(config)#host Router-A
Router-A(config)#int g0/0
Router-A(config-if)#no shutdown
Router-A(config-if)#no ip address
Router-A(config-if)#int g0/0.1
Router-A(config-subif)#encapsulation dot1Q 10
Router-A(config-subif)#ip add 192.168.10.1 255.255.255.0
Router-A(config-subif)#no shutdown
Router-A(config-subif)#int g0/0.2
Router-A(config-subif)#encapsulation dot1Q 20
Router-A(config-subif)#ip add 192.168.20.1 255.255.255.0
Router-A(config-subif)#no shutdown
```

步骤 7：测试连通性。在 PC1 上 ping PC2 的 IP 地址，网络已通，如图 3-3-2 所示。



小贴士

(1) 此时在以太网接口 fa0/0 中不要配置 IP 地址，因为这种情况下的物理接口在配置封装之后仅仅作为一个二层的链路通道存在，而不是具备三层地址的接口。

(2) 路由器中一定要创建两个 VLAN 才能进行后续配置。

(3) 测试时不可以使用 VLAN 1 的成员进行测试，单臂路由不可以使 Trunk 接口与主 VLAN 成员连通。

```

PC>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Request timed out.
Reply from 192.168.20.2: bytes=32 time=0ms TTL=127
Reply from 192.168.20.2: bytes=32 time=11ms TTL=127
Reply from 192.168.20.2: bytes=32 time=11ms TTL=127

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 11ms, Average = 7ms

PC>A

```

图 3-3-2 连通性测试效果图

相关知识

单臂路由，即在路由器上设置多个逻辑子接口，每个子接口对应一个 VLAN。每个子接口的数据在物理链路上传递时都要标记封装。对于路由器的端口，在支持子接口的同时，还必须支持 Trunk 功能。

使用单臂路由器配置 VLAN 间路由时，路由器的物理接口必须与相邻交换机的 Trunk 链路相连。在路由器上，子接口是为网络上每个唯一 VLAN 创建的。每个子接口会分配专属于其子网/VLAN 的 IP 地址，这样也便于为该 VLAN 标记帧。这样，路由器可以在流量通过 Trunk 链路返回交换机时区分不同子接口的流量。

路由器一般是基于软件处理方式来实现路由的，存在一定的延时，难以达到线速交换。所以，随着 VLAN 通信流量的增多，路由器将成为通信的瓶颈，因此，单臂路由适用于通信流量较少的情况下。

配置子接口的封装类型和所属 VLAN，使用的命令如下。

```

Router(config)#int g0/0
Router(config-if)#no shutdown
Router(config-if)#no ip address
Router(config-if)#int g0/0.1          !进入 g0/0.1 子接口
Router(config-subif)#encapsulation dot1Q 10
                                         ! 封装 Trunk 协议 dot1Q, 10 为 VLAN 号

```

学习小结

本实训重点介绍了使用路由器实现不同 VLAN 间的相互通信，在实现过程中，重点理解子接口的概念，单臂路由适用于流量比较小的情况，则如果流量比较大，容易产生瓶颈，造成网络瘫痪。

实训 4 路由器系统的备份与恢复

学习情境

海成公司的网络可以正常工作了，但发现其中一台路由器无法正常工作，经过网络管理员排错，找到了问题的所在，即这台路由器的 IOS 丢失了，但网络管理员没有备份的操作系统，很难对其进行回复。

情境分析

没有路由器的 IOS，是无法使路由器恢复为正常工作状态的，所以网络管理员只能从其



他路由器上先备份 IOS，再对无法正常工作的路由器进行系统恢复。

所需设备：

- (1) Cisco 2911 路由器 2 台。
- (2) 带超级终端应用程序的 PC 1 台。
- (3) 安装好 TFTP 软件的 PC 1 台。
- (4) Console 线 1 条。

实训拓扑结构如图 3-4-1 所示。

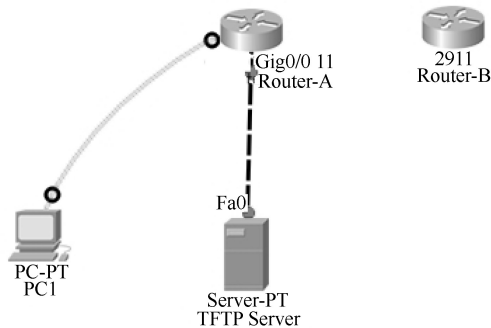


图 3-4-1 路由器系统的备份与恢复拓扑图

网络参数设置如表 3-4-1 所示。

表 3-4-1 网络参数设置

设 备	端口	IP 地址	子网掩码
Router-A	G0/0	192.168.1.1	255.255.255.0
TFTP Server		192.168.1.10	255.255.255.0

步骤实现

- 步骤 1：按照图 2-4-1 连接网络拓扑结构。
- 步骤 2：按照表 3-4-1 配置 TFTP Server 的 IP 地址、子网掩码。
- 步骤 3：配置路由器 A 的主机名称和 g0/0 接口地址。

```
Router>
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#host Router-A
Router-A(config)#int g0/0
Router-A(config-if)#ip add 192.168.1.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#
```

步骤 4：查看路由器的 IOS。

```
Router-A#show flash:
System flash directory:
File Length Name/status
3 33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
```

```
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
Router-A#
```

步骤 5: 备份路由器的 IOS。

```
Router-A#copy flash: tftp:
```

```
Source filename []? c2900-universalk9-mz.SPA.151-4.M4.bin
Address or name of remote host []? 192.168.1.10
```

```
Destination filename [c2900-universalk9-mz.SPA.151-4.M4.bin]?
```

```

Exit:  c2000_unixcell0.mz.GFA.151.4.M4.bin  |

```

[illegible][illegible]

.....

[illegible]

.....

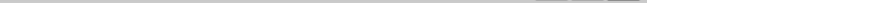
[illegible]

```
[OK - 33591768 bytes]
```

```
33591768 bytes copied in 3.546 secs (994640 bytes/sec)
Router-A#
```

步骤 6: 在 TFTP Server 中查看备份好的路由器的 IOS, 如图 3-4-2 所示。

步骤 7：将 TFTP Server 连接到要恢复 IOS 的路由器上，如图 3-4-3 所示。



Physical Config Services Desktop Software/Services

SERVICES

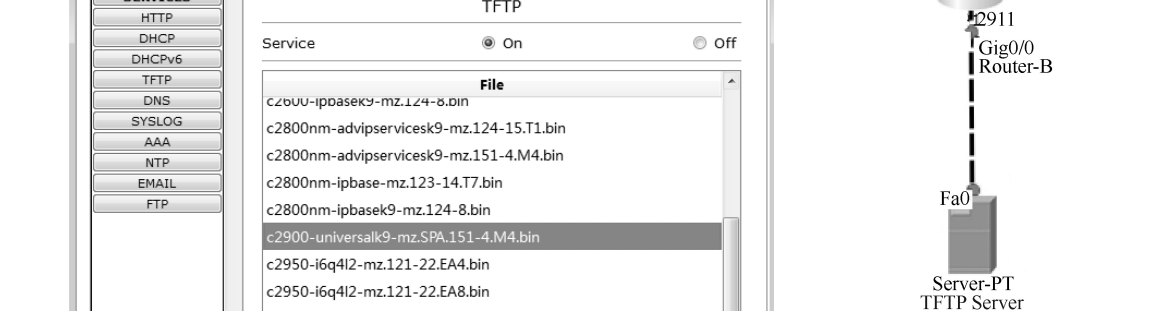
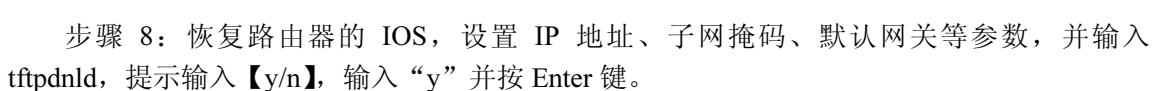


图 3-4-2 TFTP Server 界面



```
Readonly ROMMON initialized
```

```
Boot process failed...
```



```
The system is unable to boot automatically. The BOOT
environment variable needs to be set to a bootable
image.
rommon 1 > IP_ADDRESS=192.168.1.1          ! 必须要写
rommon 2 > IP_SUBNET_MASK=255.255.255.0
rommon 3 > DEFAULT_GATEWAY=192.168.1.1
rommon 4 > TFTP_SERVER=192.168.1.10
rommon 5 > TFTP_FILE=c2900-universalk9-mz.SPA.151-4.M4.bin
rommon 6 > tftpdnld      ! 按 Enter 键后，如果无法恢复，则再输入一次以上设置

IP_ADDRESS: 192.168.1.1
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 192.168.1.1
TFTP_SERVER: 192.168.1.10
TFTP_FILE: c2900-universalk9-mz.SPA.151-4.M4.bin
Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash will be lost!

Do you wish to continue? y/n: [n]:y
```

步骤 9：此时系统会恢复 IOS，完成后会出现“rommon 7>”。

```
program flash location 0x61f30000
program flash location 0x61f40000
program flash location 0x61f50000
program flash location 0x61f60000
program flash location 0x61f70000
program flash location 0x61f80000
program flash location 0x61f90000
program flash location 0x61fa0000
program flash location 0x61fb0000
program flash location 0x61fc0000
program flash location 0x61fd0000
program flash location 0x61fe0000
program flash location 0x61ff0000
program flash location 0x62000000
rommon 7 >
```

步骤 10：在“rommon 7> boot”后按 Enter 键路由器会正常进入系统。

```
rommon 7 > boot
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2911/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC
disabled
```

```

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

-----
Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image :
#####
[OK]

```

步骤 11: 查看恢复后的 IOS。

```

Router-B#show flash:

System flash directory:
File Length Name/status
6 33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
[33591768 bytes used, 222152232 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)
Router-B#

```

相关知识

TFTP 服务器可以帮助用户管理 IOS 映像的存储和对 IOS 映像的修订。对任何网络而言,最佳做法是保留 Cisco IOS 映像的副本,以防路由器中的系统映像遭到损坏或意外删除。TFTP 服务器也可用于将新的升级存储到 IOS 中,然后在需要它的网络中进行部署。

Cisco IOS 已经从用于路由的单一平台操作系统演变为支持很多功能和技术(如 VoIP、NetFlow 和 IPSec)的复杂操作系统。为了更好地满足不同的细分市场的需求,可将软件分为软件版本组和软件系列。

软件版本组包括多个 IOS 软件版本,这些软件版本共享基本代码、应用于相关硬件平台、在支持范围内会重叠(当一个 OS 生命周期终止时,会引入并支持另一个 OS)。

软件版本组中 IOS 版本的示例包括 12.3、12.4、15.0 和 15.1。

伴随每个软件版本,会创建新版本的软件以实施漏洞修复和新功能。IOS 将这些版本称为系列。

Cisco IOS 系列用于将带有通用基本代码的版本交付给一组特定的平台和功能。一个系列可能包含多个版本,每个版本是在发布时该系列基本代码的快照。由于不同的软件版本组可应用于不同的平台或细分市场,因此可以在任意时间点使用多个系列。

要在 TFTP 服务器中创建 Cisco IOS 映像的备份,可执行以下 3 个步骤。

第 1 步: 确保可以访问网络 TFTP 服务器。对 TFTP 服务器执行 ping 操作以测试连通性。

第 2 步: 验证 TFTP 服务器是否有足够的磁盘空间来容纳 Cisco IOS 映像。在路由器上使



用 `show flash0` 命令确定 Cisco IOS 映像文件的大小。

第 3 步：使用 `copy source-url destination-url` 命令将映像复制到 TFTP 服务器中。

在使用指定的源和目的 URL 发出命令后，系统将提示用户输入源文件名、远程主机的 IP 地址和目的文件名，然后开始传输。

知识拓展

如果忘记设备密码或者之前的网络管理员离职但没做好交接工作，导致新的网络管理员不知道设备密码，就需要掌握删除设备密码的相关知识。

1. 清除路由器密码

步骤 1：在路由器启动时，按 `Ctrl+break` 组合键，进入 `monitor` 模式。

```
monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

步骤 2：输入 `confreg 0x2142` 命令，并按 `Enter` 键。

```
rommon 1 > confreg 0x2142
```

步骤 3：输入 `reset` 命令，并按 `Enter` 键。

```
rommon 2 > reset
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2911/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image :
#####
[OK]
```

步骤 4：修改寄存器为正常的数值。

```
router(config)#config-register 0x2102
```

步骤 5：存盘后重启路由器。

```
router#wr
Router#reload
Proceed with reload? [confirm]
System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
```

```

Copyright (c) 2010 by cisco Systems, Inc.
Total memory size = 512 MB - On-board = 512 MB, DIMM0 = 0 MB
CISCO2911/K9 platform with 524288 Kbytes of main memory
Main memory is configured to 72/-1(On-board/DIMM0) bit mode with ECC disabled

Readonly ROMMON initialized

program load complete, entry point: 0x80803000, size: 0x1b340
program load complete, entry point: 0x80803000, size: 0x1b340

IOS Image Load Test

Digitally Signed Release Software
program load complete, entry point: 0x81000000, size: 0x3bcd3d8
Self decompressing the image :
#####
[OK]

```

学习小结

本实训介绍了路由器系统的备份与恢复，作为一名网络管理员，网络设备系统的备份与恢复是非常重要的，在恢复系统时，如果输入一次 IP 地址等参数无效，则再输入一次即可达到想要的效果。

实训 5 路由器的 DHCP 配置

DHCP 是 TCP/IP 协议簇中的一种，主要作用是给网络中其他计算机动态分配 IP 地址。

学习情境

海成公司的总经理发现自己的计算机出现了“IP 地址冲突”问题，并且联不上网络，于是找来网络管理员解决此问题，网络管理员认为是有些员工擅自修改 IP 地址导致的，可以通过在现有的三层交换机使用 DHCP 技术来解决该问题。

情境分析

网络管理员为每一台计算机手动分配一个 IP 地址，这样会大大加重网络管理员的负担，也容易导致 IP 地址分配错误，有什么办法既能减少管理员的工作量、减小输入错误的可能性，又能避免 IP 地址冲突呢？网络管理员的想法非常正确，使用 DHCP 非常方便而且在不需要增加硬件即可实现。

所需设备：

- (1) Cisco 2911 路由器 1 台。
- (2) PC 1 台。
- (3) 交叉线 1 条。
- (4) Console 线 1 条。

实训拓扑结构图 3-5-1 所示。

网络参数设置如表 3-5-1 所示。

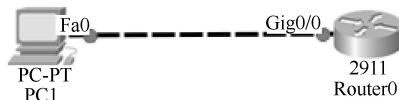


图 3-5-1 DHCP 配置拓扑图



表 3-5-1 网络参数设置

设 备	端 口	IP	子网掩码	网关
Router-A	G0/0	192.168.2.1	255.255.255.0	无
PC1		自动获取	自动获取	自动获取

步骤实现

步骤 1：按照图 3-5-1 正确连接拓扑结构。

步骤 2：按表 3-5-1 为路由器设置主机名称和接口 IP 地址。

```
Router>enable                ! 进入特权模式
Router#config terminal        ! 进入全局配置模式
Router(config)##hostname Router-A    ! 修改机器名称
Router(config)##interface g0/0      ! 进入接口模式
Router-A(config-if)#ip address 192.168.2.1 255.255.255.0    ! 配置 IP 地址
Router-A(config-if)#no shutdown
Router-A(config-if)#^Z          ! 按 Ctrl+Z 组合键进入特权模式
```

步骤 3：DHCP 服务器的配置。

```
Router-A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router-A(config)#service dhcp      ! 启动 DHCP 服务
Router-A(config)#ip dhcp excluded-address 192.168.2.100 192.168.2.150
                                   ! 排除地址
Router-A(config)#ip dhcp pool 1    ! 定义地址池
Router-A(dhcp-config)#network 192.168.2.0 255.255.255.0    ! 定义网络号
Router-A(dhcp-config)#default-router 192.168.2.1
Router-A(dhcp-config)#lease
```

步骤 4：配置 PC 及验证获得的地址。

(1) 单击 PC1，在打开的 PC1 窗口中选择“Desktop”→“IP Configuration”选项，在弹出的 IP Configuration 对话框中选中“DHCP”单选按钮，设置 PC1 的 IP 地址为动态获取，如图 3-5-2 所示。



图 3-5-2 配置 PC

(2) 此时 PC1 已经获取到 IP 地址, 如图 3-5-3 所示。

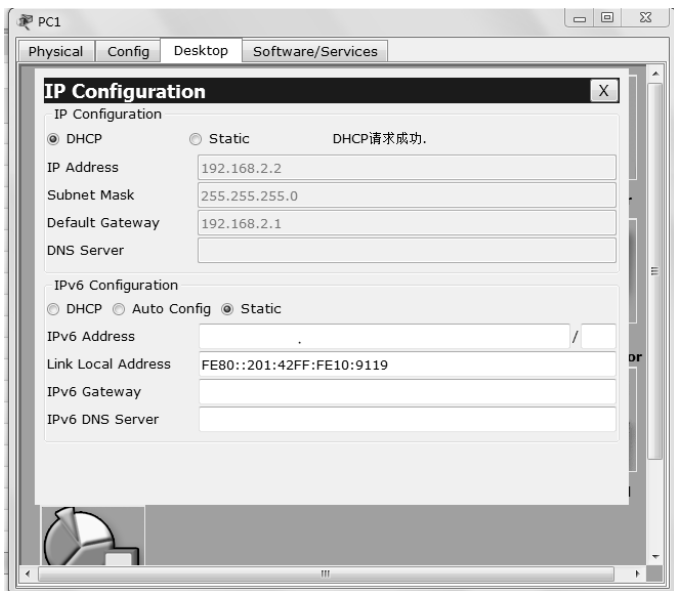


图 3-5-3 DHCP 验证效果图

步骤 5: 在路由器上验证配置。

```
Router-A#show ip dhcp binding
IP address Client-ID/ Lease expiration Type
Hardware address
192.168.2.2 0001.4210.9119 -- Automatic
Router-A#
```

相关知识

DHCP 是由服务器控制的一段 IP 地址范围, 客户机登录服务器时即可自动获得服务器分配的 IP 地址、子网掩码、网关和 DNS 地址。首先, 网络中必须存在一台 DHCP 服务器, 这个服务器可以是安装 Windows Server 2003 的计算机, 也可以是交换机或路由器设备; 其次, 客户机计算机要设置为自动获取 IP 地址的方式, 才能正常获取到 DHCP 服务器提供的 IP 地址。本实训使用三层交换机作为 DHCP 服务器进行动态分配 IP 地址。

学习小结

本实训介绍了路由器的 DHCP 服务, 可以使下连的计算机通过交换机获取 IP 地址、子网掩码、网关和 DNS 服务器地址。当一个网络中计算机数量庞大时, 使用 DHCP 服务, 可以很方便地为每一台计算机配置好相应的 IP 参数, 减轻了网络管理员分配 IP 地址的工作。

实训 6 路由器的 Telnet 配置

如果已配置好路由器的接口 IP 地址且能进行网络通信, 则可以通过局域网或广域网, 使用 Telnet 客户端登录到路由器上, 对路由器进行本地或者远程的配置。这样可以降低管理员的工作量。



学习情境

海成公司在组建局域网时，已经对公司的网络设备进行了基本配置，现在全部接入网络，投入使用。为方便对网络设备进行维护，现在需要配置其 Telnet 功能，以方便远程管理。

情境分析

Telnet 是 Cisco 交换机上支持 VTY 的默认协议。如果为 Cisco 交换机分配了管理 IP 地址，则可以使用 Telnet 客户端连接到交换机。但是 VTY 线路并不安全，可以为 VTY 线路配置密码身份验证来保护通过 VTY 线路对交换机的访问。这可以提高 Telnet 服务的安全性。

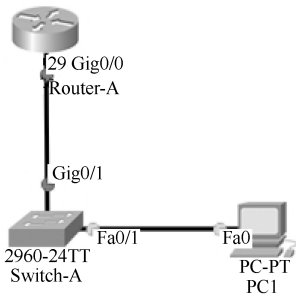


图 3-6-1 Telnet 访问路由器拓扑图

网络参数设置如表 3-6-1 所示。

所需设备：

- (1) Cisco 2911 路由器 1 台。
- (2) Cisco Catalyst 2960 交换机 1 台。
- (3) 直通线 2 条。
- (4) Console 线 1 条。

实训拓扑结构如图 3-6-1 所示

表 3-6-1 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Router-A	g0/0	192.168.1.1	255.255.255.0	无
Switch-A	VLAN1	192.168.1.100	255.255.255.0	192.168.1.1
	Fa0/1	无	无	无
	G0/1	无	无	无
PC1		192.168.1.2	255.255.255.0	192.168.1.1

步骤实现

步骤 1：按照图 3-6-1 连接网络拓扑结构。

步骤 2：按照表 3-6-1 配置计算机的 IP 地址、子网掩码和网关。

(1) 单击 PC1，在打开的 PC1 窗口中选择“Desktop”→“IP Configuration”选项，在弹出“IP Configuration”对话框中输入 IP 地址等相关信息后关闭对话框，如图 3-6-2 所示。

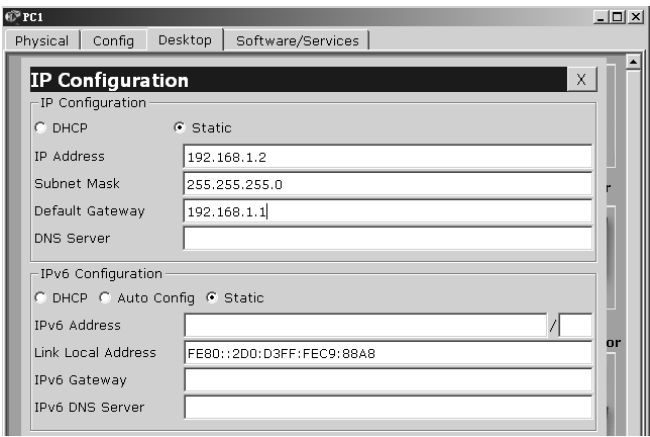


图 3-6-2 配置 PC

步骤 3：设置交换机 A 的主机名和 IP 地址。

```
Switch>
Switch>enable
Switch#conf t
Switch(config)#host Switch-A
Switch-A(config)#int vlan 1
Switch-A(config-if)#ip add 192.168.1.100 255.255.255.0
Switch-A(config-if)#exit
Switch-A(config)#ip default-gateway 192.168.1.1
Switch-A(config)#
```

步骤 4：设置路由器 A 的主机名和接口 IP 地址。

```
Router>enable
Router#configure terminal
Router(config)#host Router-A
Router-A(config)#int g0/0
Router-A(config-if)#ip add 192.168.1.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#
```

步骤 5：查看路由器 A 的端口 IP 地址配置情况。

```
Router-A#show ip int brief
Interface          IP-Address OK? Method          Status Protocol
GigabitEthernet0/0 192.168.1.1 YES manual                up up
GigabitEthernet0/1 unassigned YES unset administratively down down
GigabitEthernet0/2 unassigned YES unset administratively down down
Vlan1 unassigned YES unset administratively down down
Router-A#
```

步骤 6：设置特权模式密码。

```
Router-A#
Router-A#conf t
Router-A(config)#enable secret 123 ! 设定特权模式密码
Router-A(config)#line vty 0 4      ! 设定终端连接数为 5
Router-A(config-line)#password cisco ! 设定 Telnet 密码
Router-A(config-line)#login        ! 设定要求登录
Router-A(config-line)#
```

步骤 7：配置 Telnet。

```
Router-A(config)#username zwk password 123456
                        ! 定义 Telnet 用户名为“zwk”，密码为“123456”
Router-A(config)#line vty 0 4
Router-A(config-line)#login local
Router-A(config-line)#
```

步骤 8：保存设置。

```
Router-A#write ! 保存配置
Saving current configuration...
OK!
```



步骤 9：Telnet 测试。

(1) 单击 PC1，在打开的 PC1 窗口中选择“Desktop”→“Command Prompt”选项，弹出“Command Prompt”对话框，如图 3-6-3 所示。

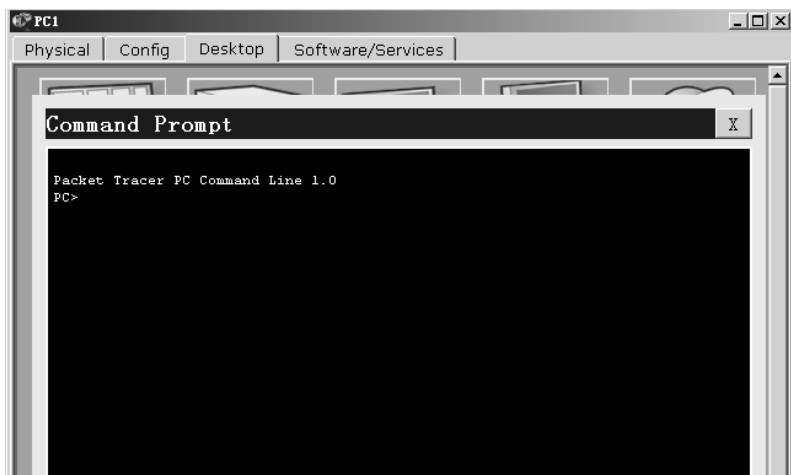


图 3-6-3 “Command Prompt”对话框

(2) 在图 3-5-3 所示对话框中，输入“telnet 192.168.1.1”后按 Enter 键，如图 3-6-4 所示。

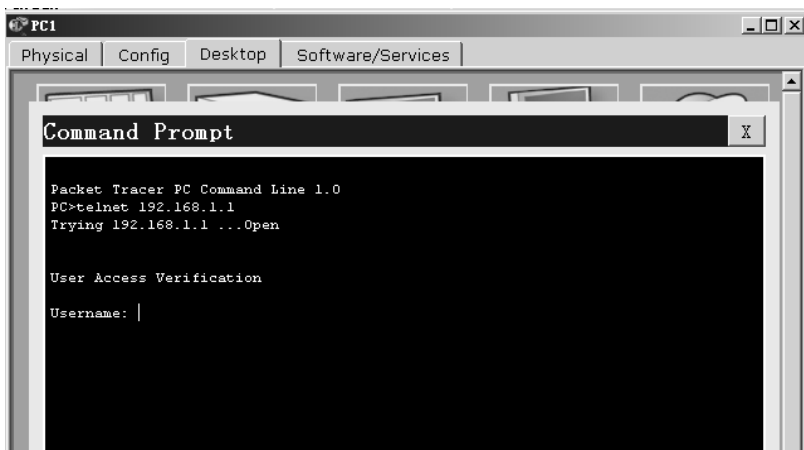


图 3-6-4 连接远程路由器

(3) 在“Username”处输入“zww”后按 Enter 键，在“Password”处输入“123456”，如图 3-6-5 所示，出现“Router>”表示远程登录成功。



小贴士

(1) CR-V35FC 所连接的接口为 DCE，需要配置时钟频率，CR-V35MT 所连接的接口为 DTE。

(2) 查看接口状态，如果接口是 DOWN，通常是线缆出现了故障；如果协议是 DOWN，通常是因为时钟频率没有配置，或者两端封装协议不一致。

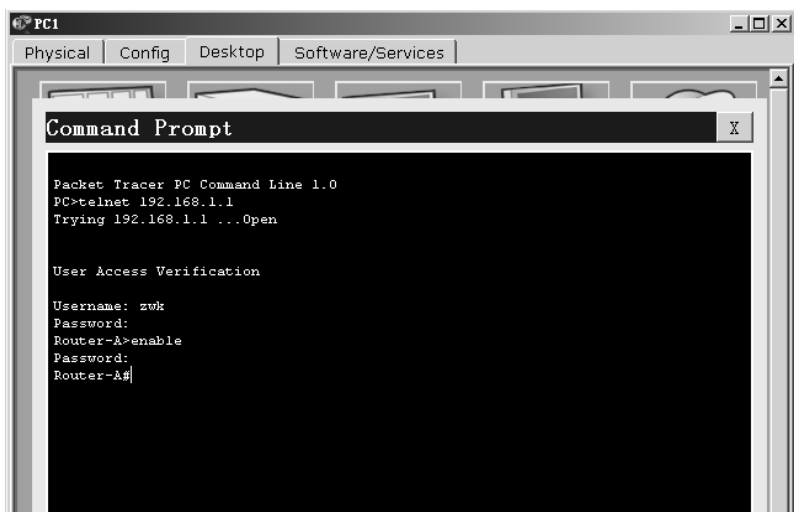


图 3-6-5 Telnet 路由器效果图

相关知识

远程访问思科网络设备的 VTY 接口有两种选择：Telnet 与 SSH。

Telnet 是早期型号的 Cisco 路由器上支持的方法。Telnet 是用于终端访问的常用协议，因为大部分最新的操作系统都附带内置的 Telnet 客户端。但是 Telnet 不是访问网络设备的安全方法，因为它在网络上以明文发送所有通信。攻击者使用网络监视软件可以读取 Telnet 客户端和 Cisco 路由器的 Telnet 服务之间发送的每一个字符。由于 Telnet 协议存在安全性问题，因此 SSH 成为用于远程访问 Cisco 设备虚拟终端线路的首选协议。

SSH 提供与 Telnet 相同类型的访问，但是增加了安全性。SSH 客户端和 SSH 服务器之间的通信是加密的。SSH 已经经历了多个版本，Cisco 设备目前支持 SSHv1 和 SSHv2。建议尽可能实施 SSHv2，因为它使用了比 SSHv1 更强的安全加密算法。

知识拓展

1. 配置路由器为 SSH 服务器

SSH 功能有 SSH 服务器和 SSH 集成客户端，后者是在路由器上运行的应用程序。可以使用 PC 上运行的任意 SSH 客户端或交换机上运行的 Cisco SSH 客户端来连接运行 SSH 服务器的服务器。

对于服务器组件，路由器同样支持 SSHv1 或 SSHv2。

所需设备：

- (1) Cisco 2911 路由器 1 台。
- (2) Cisco Catalyst 2960 交换机 1 台。
- (3) 直通线 2 条。
- (4) Console 线 1 条。

此实验拓扑结构如图 3-6-6 所示。

网络参数配置如表 3-6-2 所示。

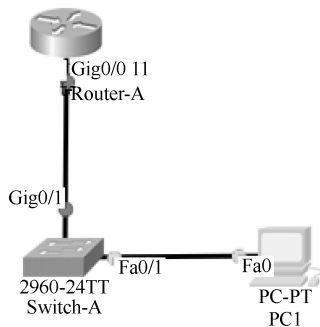


图 3-6-6 SSH 访问路由器拓扑



表 3-6-2 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Router-A	G0/0	192.168.1.1	255.255.255.0	无
Switch-A	VLAN 1	192.168.1.100	255.255.255.0	192.168.1.1
	Fa0/1	无	无	无
	G0/1	无	无	无
PC1		192.168.1.2	255.255.255.0	192.168.1.1

步骤实现

步骤 1：按照图 3-6-6 连接网络拓扑结构。

步骤 2：按照表 3-6-2 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：设置交换机 A 的主机名和 IP 地址。

```
Switch>
Switch>enable
Switch#conf t
Switch(config)#host Switch-A
Switch-A(config)#int vlan 1
Switch-A(config-if)#ip add 192.168.1.100 255.255.255.0
Switch-A(config-if)#exit
Switch-A(config)#ip default-gateway 192.168.1.1
Switch-A(config)#
```

步骤 4：设置路由器 A 的主机名和接口 IP 地址。

```
Router>enable
Router#configure terminal
Router(config)#host Router-A
Router-A(config)#int g0/0
Router-A(config-if)#ip add 192.168.1.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#
```

步骤 5：查看路由器 A 的端口 IP 地址配置情况。

```
Router-A#show ip int brief
Interface                IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0      192.168.1.1     YES manual    up              up
GigabitEthernet0/1      unassigned      YES unset     administratively dom down
GigabitEthernet0/2      unassigned      YES unset     administratively dom down
Vlan1                    unassigned      YES unset     administratively dom down
Router-A# |
```

步骤 6：设置特权模式的密码。

```
Router-A#
Router-A#conf t
Router-A(config)#enable secret 123456    ! 设定特权模式密码
Router-A(config)#
```

步骤 7: 配置 SSH 服务器。

```
Router-A(config)#ip domain-name abc.com
Router-A(config)#username zwk password cisco
                        ! 定义 Telnet 用户名为“zwk”，密码为“cisco”
Router-A(config)#line vty 0 15      ! 设定终端连接数为 16
Router-A(config-line)#transport input ssh
Router-A(config-line)#login local    ! 设定要求登录
Router-A(config-line)#exit
Router-A(config)#crypto key generate rsa
The name for the keys will be: Router-A.abc.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

步骤 8: 配置 SSH 路由器服务器的版本为第 2 版。

```
Router-A(config)#
Router-A(config)#ip ssh version 2
```

步骤 9: 保存设置。

```
Router-A#write                                ! 保存配置
Saving current configuration...
OK!
```

步骤 10: SSH 测试。

(1) 单击 PC1 在打开的 PC1 窗口中选择“Desktop”→“Command Prompt”选项，弹出“Command Prompt”对话框，如图 3-6-7 所示。

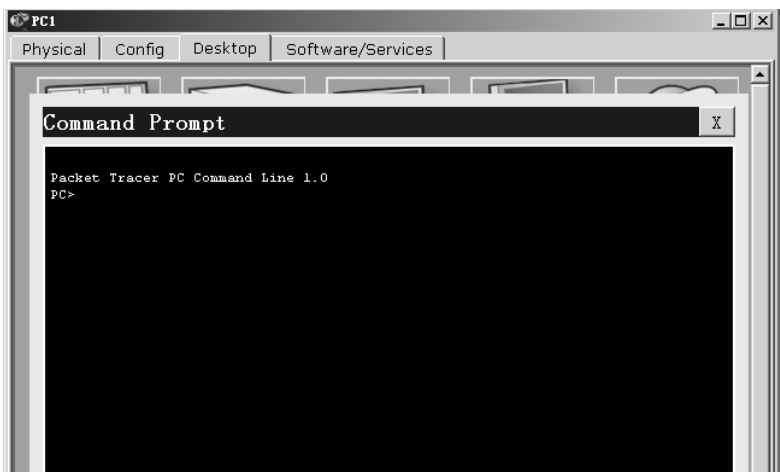


图 3-6-7 “Command Prompt”对话框

(2) 在图 3-6-7 所示对话框中，输入“SSH -l zwk 192.168.1.1 ”命令后按 Enter 键，如图 3-6-8 所示。

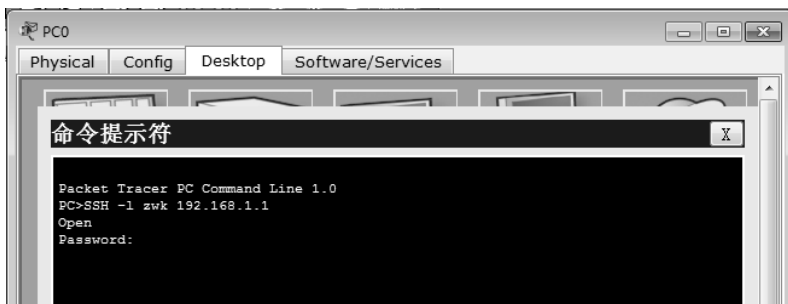


图 3-6-8 连接远程 SSH 路由器

(3) 在“Password”处输入“cisco”，如图 3-6-9 所示，出现“Router-A>”表示远程登录成功。

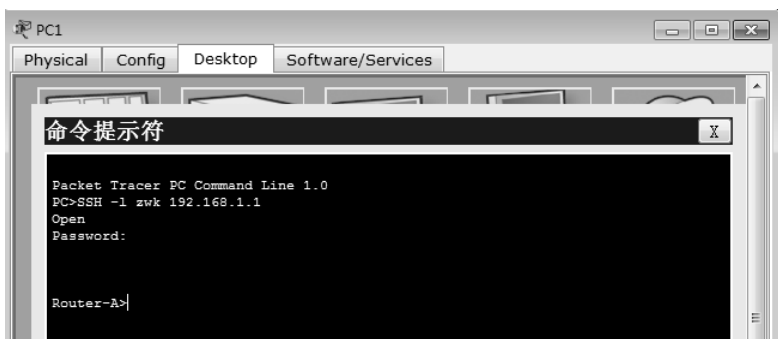


图 3-6-9 SSH 路由器效果图

学习小结

本实训介绍了如何在路由器上实现 Telnet 和 SSH，这对网络管理员来说是至关重要的，因为可以在很大程度上方便管理员的工作，要注意 Telnet 和 SSH 的区别，实际工作中使用 SSH 更多一些，因为 Telnet 是明文传输的，而 SSH 是密文传输的，SSH 相对来说更安全。

项目考核

某公司规模很小，只有 3 个 VLAN，分别为 VLAN 10、VLAN 20 和 VLAN 30，如图 3-6-10 所示，要实现全网互通，VLAN 30 是动态获取 IP 地址的，并能在 PC1 上实现远程访问公司的路由器和交换机。

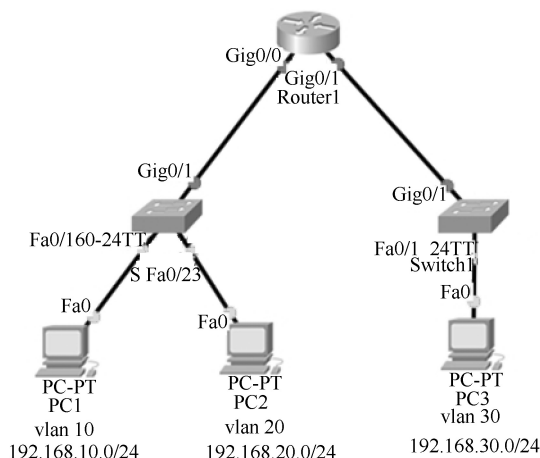
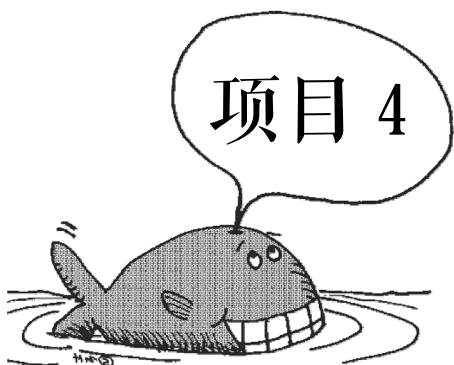


图 3-6-10 某公司网络拓扑图



路由协议实现

项目学习说明

路由器提供了异构网互连的机制，可实现将一个网络的数据包发送到另一个网络。而路由就是指导 IP 数据包发送的路径信息。路由协议就是在路由指导 IP 数据包发送过程中事先约定好的规定和标准。路由协议通过在路由器之间共享路由信息来支持可路由协议。路由信息在相邻路由器之间传递，确保所有路由器知道到其他路由器的路径。总之，路由协议创建了路由表，描述了网络拓扑结构；路由协议与路由器协同工作，执行路由选择和数据包转发功能。在实际应用中路由器通常连接着许多不同的网络，要实现多个不同网络间的通信，则要在路由器上配置路由协议。

本项目重点学习路由器的静态路由配置、路由器的动态路由配置。

学习能力目标

实训 1：静态路由配置。

实训 2：动态路由配置。

职业能力目标

能实现路由器和三层交换机的静态路由协议。

能实现路由器和三层交换机的默认路由协议。

能实现路由器和三层交换机的动态路由协议。



实训 1 静态路由配置

静态路由是指由网络管理员手工配置的路由信息。当网络的拓扑结构或链路状态发生变化时，网络管理员要手工修改路由表中的静态路由信息。静态路由信息在默认情况下不会传递给其他路由器。静态路由一般适用于比较简单的网络环境。

学习情境

海成公司刚成立，规模很小，只有 2 台路由器和 1 台三层交换机。该公司的网络管理员经过考虑，决定在公司的路由器、交换机与运营商路由器之间使用静态路由，实现网络的互连。

情境分析

由于该网络规模较小且不经常变动，所以使用静态路由比较合适。两台路由器之间通过以太网口相连，每台路由器连接一台计算机。

所需设备：

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco 3560-24PS 交换机 1 台。
- (3) PC 3 台。
- (4) 交叉线 2 条。
- (5) 直通线 2 条。
- (6) DCE 串口和 DTE 串口线 1 条。
- (7) Console 线 1 条。

实训拓扑结构如图 4-1-1 所示。

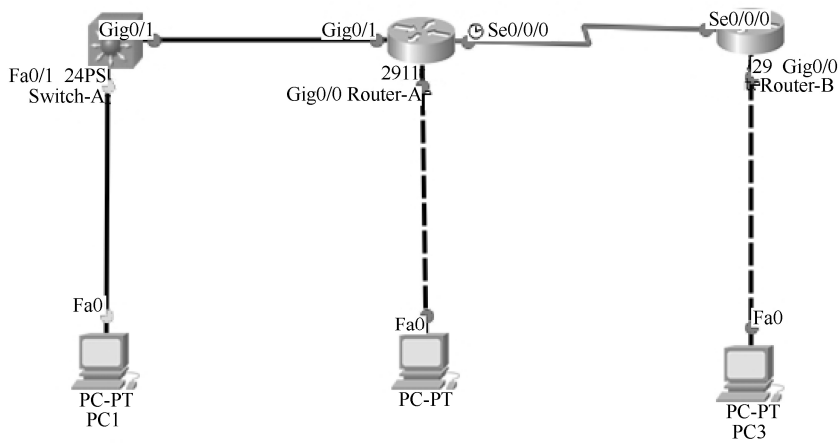


图 4-1-1 静态路由拓扑图

网络参数设置如表 4-1-1 所示。

表 4-1-1 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Switch-A	G0/1	192.168.1.1	255.255.255.0	无
	F0/1	192.168.10.1	255.255.255.0	无

(续表)

设 备	端 口	IP 地址	子网掩码	网关 1
Router-A	G0/1	192.168.1.2	255.255.255.0	无
	G0/0	192.168.20.1	255.255.255.0	无
	S0/0/0	192.168.2.1	255.255.255.0	无
Router-B	S0/0/0	192.168.2.2	255.255.255.0	无
	G0/0	192.168.30.1	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1
PC3		192.168.30.2	255.255.255.0	192.168.30.1

步骤实现

步骤 1：按照图 4-1-1 连接网络拓扑结构。

步骤 2：按照表 4-1-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置 Switch-A 的名称及其接口 IP 地址。

```
Switch>
Switch>en
Switch#conf t
Switch(config)#host Switch-A
Switch-A(config)#ip routing
Switch-A(config)#int fa0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.10.1 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config-if)#int g0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.1.1 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config-if)#
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router>enable
Router#conf t
Router(config)#host Router-A
Router-A(config)#int g0/1
Router-A(config-if)#ip add 192.168.1.2 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int g0/0
Router-A(config-if)#ip add 192.168.20.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int s0/0/0
Router-A(config-if)#clock rate 64000
Router-A(config-if)#ip add 192.168.2.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#
```



步骤 5：配置 Router-B 的名称及其接口 IP 地址。

```
Router>en
Router#conf t
Router(config)#host Router-B
Router-B(config)#int g0/0
Router-B(config-if)#ip add 192.168.30.1 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#int s0/0/0
Router-B(config-if)#ip add 192.168.2.2 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#
```

步骤 6：查看 Switch-A 接口的配置情况。

```
Switch-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	192.168.10.1	YES	manual	up	up
GigabitEthernet0/1	192.168.10.1	YES	manual	up	up

步骤 7：查看 Router-A 接口的配置情况。

```
Router-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.20.1	YES	manual	up	up
GigabitEthernet0/1	192.168.1.2	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Serial10/0/0	192.168.2.1	YES	manual	up	up
Serial10/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router-A#
```

步骤 8：查看 Router-B 接口的配置情况。

```
Router-B#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.30.2	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Serial10/0/0	192.168.2.2	YES	manual	up	up
Serial10/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router-B#
```

步骤 9：查看 Router-A 的路由表。

```
Router-A#show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.2/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
Router-A#
```

步骤 10: 查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.2/32 is directly connected, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0
L 192.168.30.2/32 is directly connected, GigabitEthernet0/0
Router-B#
```

步骤 11: 查看 Switch-A 的路由表。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
```



```
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
C 192.168.10.0/24 is directly connected, FastEthernet0/1
Switch-A#
```

步骤 12: 配置路由协议前, 使用 ping 命令测试网络的连通性。在 PC 1 上 ping PC 2 和 PC 3 的 IP 地址, 网络未连通, 如图 4-1-2 所示。

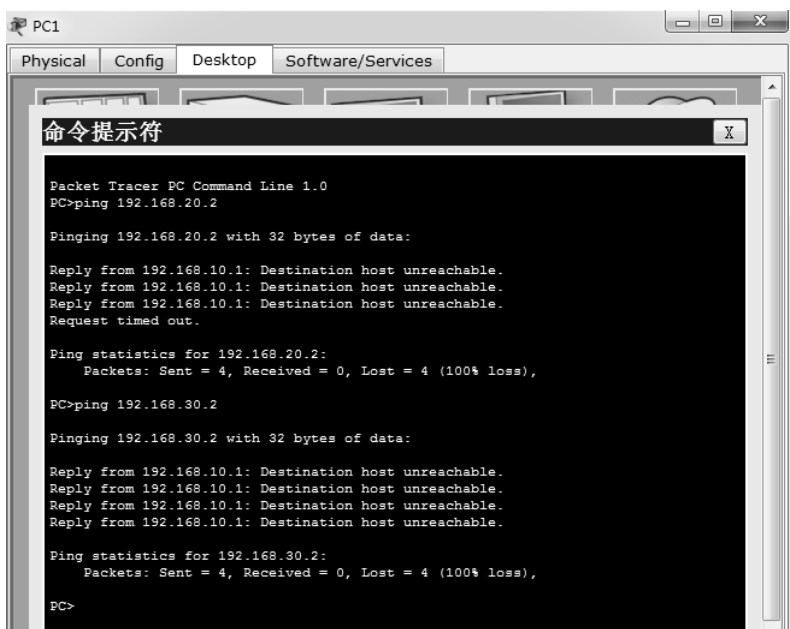


图 4-1-2 连通性测试效果图（未连通）

步骤 13: 在 Switch-A 上配置静态路由。

```
Switch-A#
Switch-A#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch-A(config)#ip route 192.168.20.0 255.255.255.0 192.168.1.2
Switch-A(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2
Switch-A(config)#ip route 192.168.30.0 255.255.255.0 192.168.1.2
Switch-A(config)#
```

步骤 14: 在 Router-A 上配置静态路由。

```
Router-A#conf t
Router-A(config)#ip route 192.168.10.0 255.255.255.0 192.168.1.1
Router-A(config)#ip route 192.168.30.0 255.255.255.0 192.168.2.2
Router-A(config)#
```

步骤 15: 在 Router-B 上配置静态路由。

```
Router-B#conf t
Router-B(config)#ip route 192.168.10.0 255.255.255.0 192.168.2.1
```

```
Router-B(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1
Router-B(config)#ip route 192.168.20.0 255.255.255.0 192.168.2.1
Router-B(config)#
```

步骤 16: 查看 Switch-A 的路由表。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
S 192.168.2.0/24 [1/0] via 192.168.1.2
C 192.168.10.0/24 is directly connected, FastEthernet0/1
S 192.168.20.0/24 [1/0] via 192.168.1.2
S 192.168.30.0/24 [1/0] via 192.168.1.2
```

Switch-A#

步骤 17: 查看 Router_A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.2/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
S 192.168.10.0/24 [1/0] via 192.168.1.1
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
S 192.168.30.0/24 [1/0] via 192.168.2.2
```

Router-A#

! 注意, 静态路由的管理距离是 1



步骤 18: 查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

S 192.168.1.0/24 [1/0] via 192.168.2.1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.2/32 is directly connected, Serial0/0/0
S 192.168.10.0/24 [1/0] via 192.168.2.1
S 192.168.20.0/24 [1/0] via 192.168.2.1
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0
L 192.168.30.2/32 is directly connected, GigabitEthernet0/0
Router-B#
```

！注意，静态路由的管理距离是 1

步骤 19: 配置路由协议后，验证网络的连通性。在 PC 1 上 ping PC 2 和 PC 3 的 IP 地址，网络已连通，如图 4-1-3 所示。

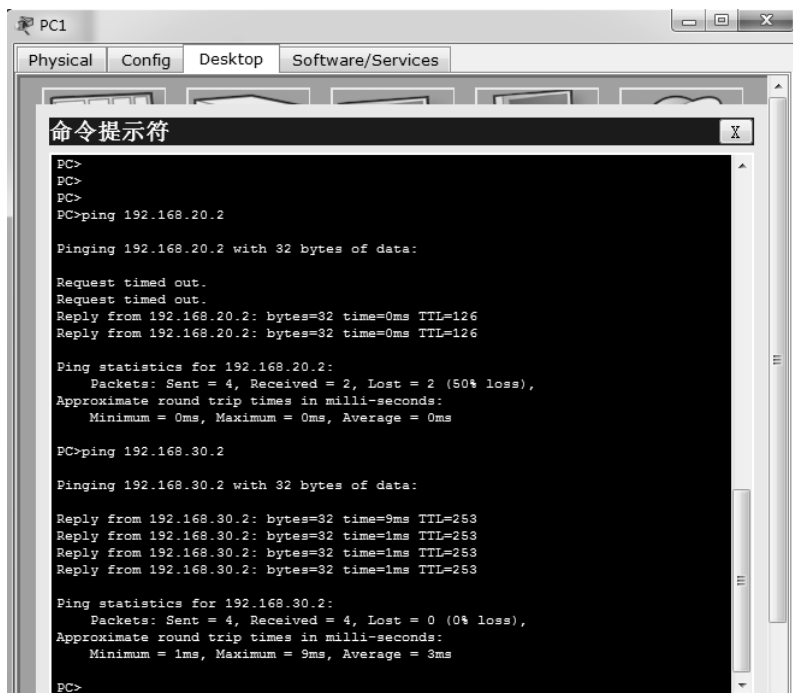


图 4-1-3 连通性测试效果图（连通）



小贴士

- (1) 在配置静态路由时，必须双向配置才能连通。
- (2) 非直连的网段都要配置路由。
- (3) 两台路由器如果使用串口连接，则必须将其中一端设置为 DCE 端。

相关知识

1. 路由表的产生方式

路由器或三层交换机在转发数据时，首先要在路由表中查找相应的路由。路由表的产生方式有如下 3 种。

- (1) 直连网络：路由器或三层交换机自动添加和自己直接连接的网络路由。
- (2) 静态路由：由网络管理员手工配置的路由信息。当网络的拓扑结构或链路发生变化时，需要网络管理员手动修改路由表中的相关路由信息。
- (3) 动态路由：由路由协议动态产生的路由。

2. 静态路由的优缺点

静态路由的优点：使用静态路由的好处是网络安全保密性高。动态路由因为需要路由器之间频繁地交换各自的路由表，而对路由表的分析可以揭示网络的拓扑结构和网络地址等信息。因此，出于网络安全方面的考虑可以采用静态路由。

静态路由的缺点：大型和复杂的网络环境通常不宜采用静态路由。一方面，网络管理员难以全面地了解整个网络的拓扑结构；另一方面，当网络的拓扑结构和链路状态发生变化时，路由器中的静态路由信息需要大范围地调整，这一工作的难度和复杂程度非常高。

在小型的网络中，使用静态路由是较好的选择，管理员想控制数据转发路径时，也可使用静态路由。

静态路由的配置命令如下。

```
ip route 目的网络的 IP 地址 子网掩码 下一跳 IP 地址/本地接口
```

三层交换机实现路由的方法如下。

```
Switch-A(config)#ip routing          ! 开启路由功能
Switch-A(config-if)#int g0/1
Switch-A(config-if)#no switchport    ! 关闭端口的交换功能
Switch-A(config-if)#ip add 192.168.1.1 255.255.255.0
```

知识拓展

默认路由是一种特殊的静态路由，指的是当路由表中与包的目的地址之间没有匹配的表项时路由器能够做出的选择。如果没有默认路由，那么目的地址在路由表中没有匹配表项的包将被丢弃。默认路由在某些时候非常有效，当存在末梢网络时，默认路由会大大简化路由器的配置，减轻网络管理员的工作负担，提高网络性能。

默认路由和静态路由的命令格式一样。只是把目的 IP 地址和子网掩码改为了 0.0.0.0 和 0.0.0.0。默认路由的配置命令如下。

```
ip route 0.0.0.0 0.0.0.0 下一跳 IP 地址
```

配置默认路由如图 4-1-4 所示。

网络参数设置如表 4-1-2 所示。

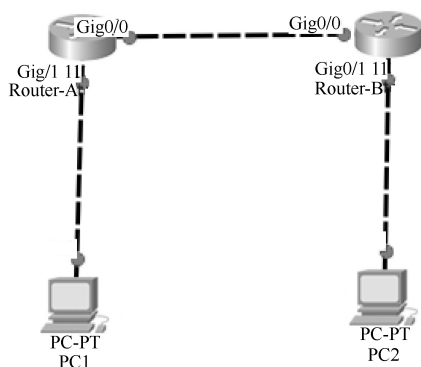


图 4-1-4 默认路由拓扑图

表 4-1-2 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Router-A	G0/0	192.168.1.1	255.255.255.0	无
	G0/1	192.168.10.1	255.255.255.0	无
Router-B	G0/0	192.168.1.2	255.255.255.0	无
	G0/1	192.168.20.1	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1

步骤实现

步骤 1：按照图 4-1-4 连接网络拓扑结构。

步骤 2：按照表 4-1-2 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置 Router-A 的名称及其接口 IP 地址。

```
Router>en
Router#conf t
Router(config)#host Router-A
Router-A(config)#int g0/0
Router-A(config-if)#ip add 192.168.1.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int g0/1
Router-A(config-if)#ip add 192.168.10.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#^Z
Router-A#
```

步骤 4：配置 Router-B 的名称及其接口 IP 地址。

```
Router>en
Router#conf t
Router(config)#host Router-B
Router-B(config)#int g0/0
Router-B(config-if)#ip add 192.168.1.2 255.255.255.0
Router-B(config-if)#no shut
```

```
Router-B(config-if)#int g0/1
Router-B(config-if)#ip add 192.168.20.1 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#^Z
Router-B#
```

步骤 5: 查看 Router-A 接口的配置情况。

```
Router-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.1	YES	manual	up	up
GigabitEthernet0/1	192.168.10.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router-A#
```

步骤 6: 查看 Router-B 接口的配置情况。

```
Router-B#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.1.2	YES	manual	up	up
GigabitEthernet0/1	192.168.20.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router-B#
```

步骤 7: 查看 Router-A 的路由表。

```
Router-A#show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1
Router-A#
```

步骤 8: 查看 Router-B 的路由表。

```
Router-B#show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area



```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.2/32 is directly connected, GigabitEthernet0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/1
L 192.168.20.1/32 is directly connected, GigabitEthernet0/1
Router-B#
```

步骤 9：配置路由协议前，使用 ping 命令测试网络的连通性。

(1) 在 PC 1 上 ping PC 2 的 IP 地址 192.168.20.2，网络未连通，如图 4-1-5 所示。

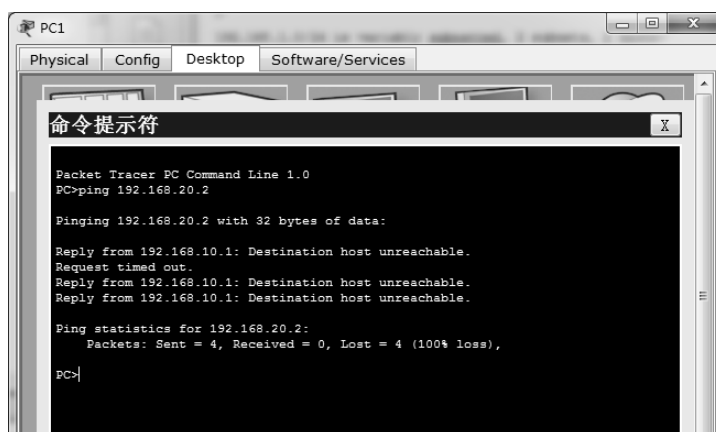


图 4-1-5 连通性测试效果图（一）

(2) 在 PC 2 上 ping PC 1 的 IP 地址 192.168.10.2，网络未连通，如图 4-1-6 所示。

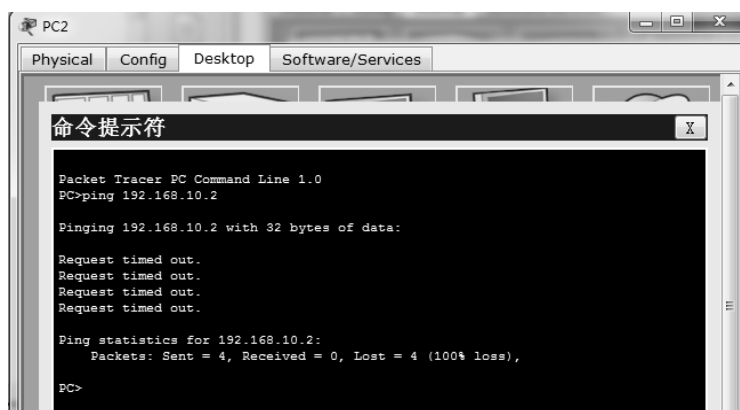


图 4-1-6 连通性测试效果图（二）

步骤 10: 在 Router-A 上配置默认路由。

```
Router-A#
Router-A#conf t
Router-A(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2
Router-A(config)#
```

步骤 11: 在 Router-B 上配置默认路由。

```
Router-#
Router-B#conf t
Router-B(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.1
Router-B(config)#
```

步骤 12: 查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.1.2 to network 0.0.0.0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 192.168.1.2
Router-A#
```

步骤 13: 查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 192.168.1.12 to network 0.0.0.0

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
```



```
L 192.168.1.2/32 is directly connected, GigabitEthernet0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/1
L 192.168.20.1/32 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 192.168.1.12
[1/0] via 192.168.1.1
Router-B#
```

步骤 14: 配置路由协议后，使用 ping 命令验证网络的连通性。

(1) 在 PC 1 上 ping PC 2 的 IP 地址 192.168.20.2，网络已连通，如图 4-1-7 所示。

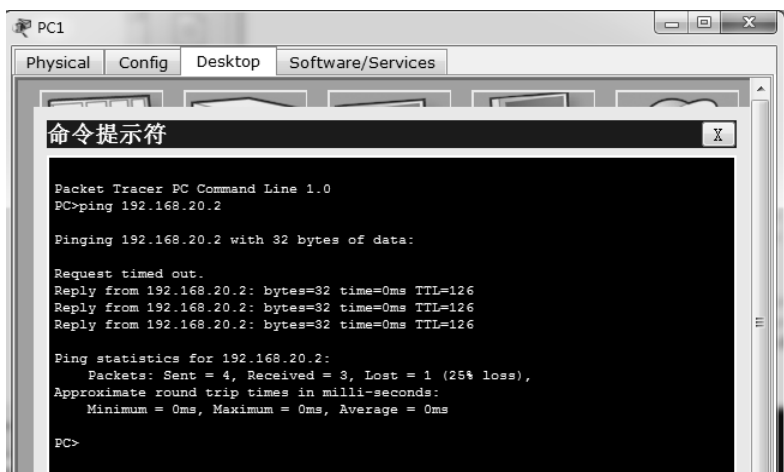


图 4-1-7 连通性测试效果图（三）

(2) 在 PC 2 上 ping PC 1 的 IP 地址 192.168.10.2，网络已连通，如图 4-1-8 所示。

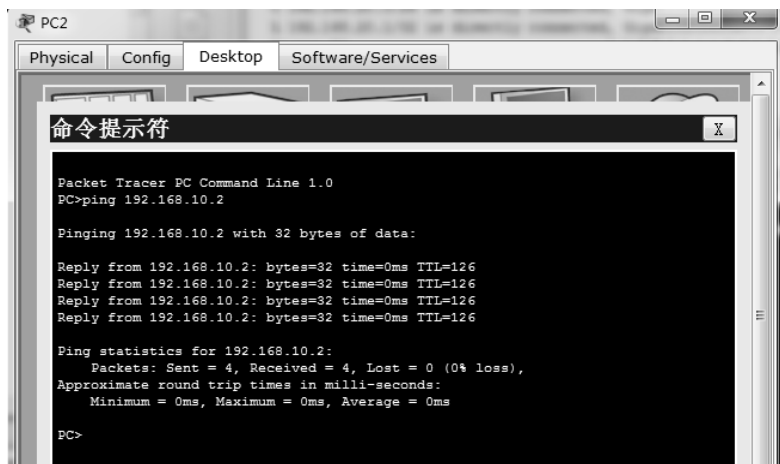


图 4-1-8 连通性测试效果图（四）

学习小结

本实训介绍了路由器、三层交换机之间如何实现静态路由，需要注意的是，添加静态路由时非直连网段也要进行配置。静态路由开销小，但不灵活，只适用于相对稳定的网络。在小型网络环境中，选择静态路由是不错的，但对于大中型网络，静态路由就不适用了。

实训 2 动态路由配置

在路由器较多的网络环境中，手工配置静态路由会给管理员带来很重的工作负担，使用动态路由协议可以很好地解决此问题。

任务 1 RIP 动态路由配置

路由信息协议（Routing Information Protocol, RIP）是应用较早、使用较普遍的动态路由协议，也是内部网关协议，由于 RIP 以跳数作为衡量路径的开销，且规定最大跳数为 15，因此 RIP 在实际应用中是有一定限制的，通常适用于中小型企业网络。

学习情境

海成公司由于规模的不断扩大，路由器和三层交换机的数量已经达到了 5 台。该公司的网络管理员发现原有的静态路由已经不适合现在的公司，因此，决定在公司的路由器之间使用动态的 RIP 路由协议，实现网络的互连。

情境分析

由于公司的网络规模开始扩大，网路管理员发现使用静态路由确实不合适，所以决定使用动态的 RIP 路由协议。

所需设备：

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco 3560-24PS 交换机 1 台。
- (3) PC 3 台。
- (4) 交叉线 2 条。
- (5) 直通线 2 条。
- (6) DCE 串口和 DTE 串口线 1 条。
- (7) Console 线 1 条。

任务拓扑结构如图 4-2-1 所示。

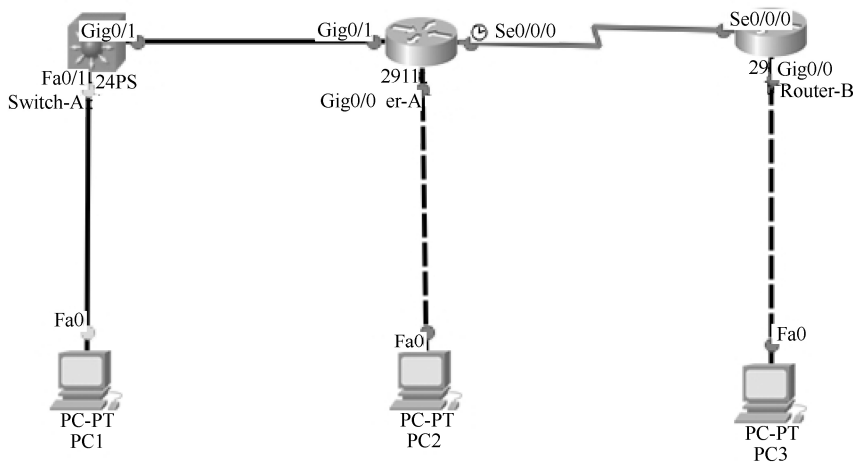


图 4-2-1 利用 RIP 实现网络的连通



网络参数设置如表 4-2-1 所示。

表 4-2-1 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Switch-A	G0/1	192.168.1.1	255.255.255.0	无
	F0/1	192.168.10.1	255.255.255.0	无
Router-A	G0/1	192.168.1.2	255.255.255.0	无
	G0/0	192.168.20.1	255.255.255.0	无
	S0/0/0	192.168.2.1	255.255.255.0	无
Router-B	S0/0/0	192.168.2.2	255.255.255.0	无
	G0/0	192.168.30.1	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1
PC3		192.168.30.2	255.255.255.0	192.168.30.1

步骤实现

步骤 1：按照图 4-2-1 连接网络拓扑结构。

步骤 2：按照表 4-2-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置 Switch-A 的名称及其接口 IP 地址。

```
Switch>
Switch>en
Switch#conf t
Switch(config)#host Switch-A
Switch-A(config)#int fa0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.10.1 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config-if)#int g0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.1.1 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config-if)#exit
Switch-A(config)#ip routing
Switch-A(config)#
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router>enable
Router#conf t
Router(config)#host Router-A
Router-A(config)#int g0/1
Router-A(config-if)#ip add 192.168.1.2 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int g0/0
Router-A(config-if)#ip add 192.168.20.1 255.255.255.0
Router-A(config-if)#no shut
```

```
Router-A(config-if)#int s0/0/0
Router-A(config-if)#clock rate 64000
Router-A(config-if)#ip add 192.168.2.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#
```

步骤 5: 配置 Router-B 的名称及其接口 IP 地址。

```
Router>en
Router#conf t
Router(config)#host Router-B
Router-B(config)#int g0/0
Router-B(config-if)#ip add 192.168.30.1 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#int s0/0/0
Router-B(config-if)#ip add 192.168.2.2 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#
```

步骤 6: 查看 Switch-A 的接口配置情况。

```
Switch-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	192.168.10.1	YES	manual	up	up
GigabitEthernet0/1	192.168.10.1	YES	manual	up	up

步骤 7: 查看 Router-A 的接口配置情况。

```
Router-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.20.1	YES	manual	up	up
GigabitEthernet0/1	192.168.1.2	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Serial0/0/0	192.168.2.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

Router-A#

步骤 8: 查看 Router-B 的接口配置情况。

```
Router-B#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.30.2	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Serial0/0/0	192.168.2.2	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

Router-B#

步骤 9: 查看 Router-A 的路由表。

```
Router-A#show ip route
```




```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.2/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
Router-A#
```

步骤 10: 查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.2/32 is directly connected, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0
L 192.168.30.2/32 is directly connected, GigabitEthernet0/0
Router-B#
```

步骤 11: 查看 Switch-A 的路由表。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```

E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1

C 192.168.10.0/24 is directly connected, FastEthernet0/1

Switch-A#

步骤 12: 配置路由协议前, 使用 ping 命令测试网络的连通性。

(1) 在 PC 1 上 ping PC 2 和 PC 3 的 IP 地址, 网络未连通, 如图 4-2-2 所示。

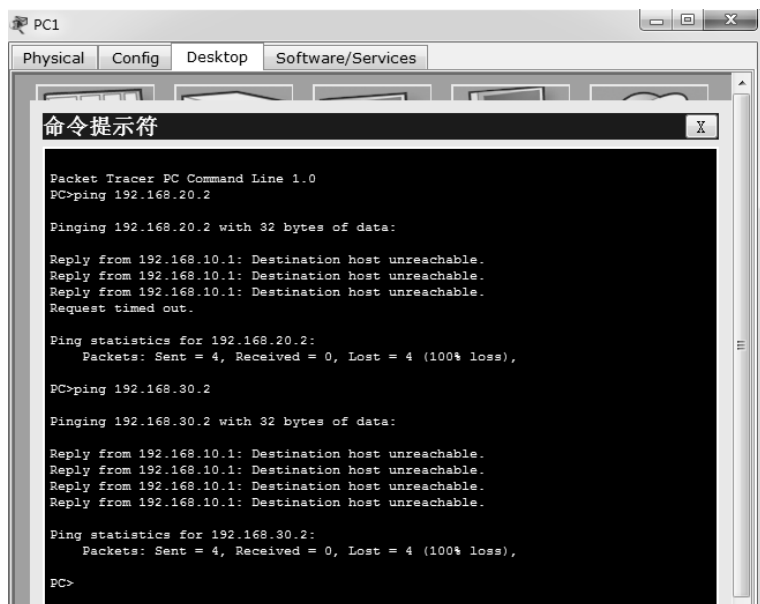


图 4-2-2 连通性测试效果图 (一)

步骤 13: 在 Switch-A 上配置动态 RIP。

```

Switch-A#conf t
Switch-A(config)#router rip
Switch-A(config-router)#network 192.168.10.0
Switch-A(config-router)#network 192.168.1.0
Switch-A(config-router)#

```

步骤 14: 在 Router-A 上配置动态 RIP。

```

Router-A#
Router-A#conf t
Router-A(config)#router rip
Router-A(config-router)#network 192.168.1.0
Router-A(config-router)#network 192.168.20.0
Router-A(config-router)#network 192.168.2.0
Router-A(config-router)#

```



步骤 15: 在 Router-B 上配置动态 RIP。

```
Router-B#conf t
Router-B(config)#router rip
Router-B(config-router)#network 192.168.2.0
Router-B(config-router)#network 192.168.30.0
Router-B(config-router)#
```

步骤 16: 查看 Switch-A 的路由表。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
R 192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:02, GigabitEthernet0/1
C 192.168.10.0/24 is directly connected, FastEthernet0/1
R 192.168.20.0/24 [120/1] via 192.168.1.2, 00:00:02, GigabitEthernet0/1
R 192.168.30.0/24 [120/2] via 192.168.1.2, 00:00:02, GigabitEthernet0/1
Switch-A#
```

步骤 17: 查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.2/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
R 192.168.10.0/24 [120/1] via 192.168.1.1, 00:00:15, GigabitEthernet0/1
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
```

```
R 192.168.30.0/24 [120/1] via 192.168.2.2, 00:00:23, Serial0/0/0
Router-A#
```

步骤 18: 查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

R 192.168.1.0/24 [120/1] via 192.168.2.1, 00:00:03, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.2/32 is directly connected, Serial0/0/0
R 192.168.10.0/24 [120/2] via 192.168.2.1, 00:00:03, Serial0/0/0
R 192.168.20.0/24 [120/1] via 192.168.2.1, 00:00:03, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0
L 192.168.30.2/32 is directly connected, GigabitEthernet0/0
Router-B#
```

步骤 19: 配置路由协议后, 使用 ping 命令验证网络的连通性。

(1) 在 PC 1 上 ping PC 2 和 PC 3 的 IP 地址, 网络已连通, 如图 4-2-3 所示。

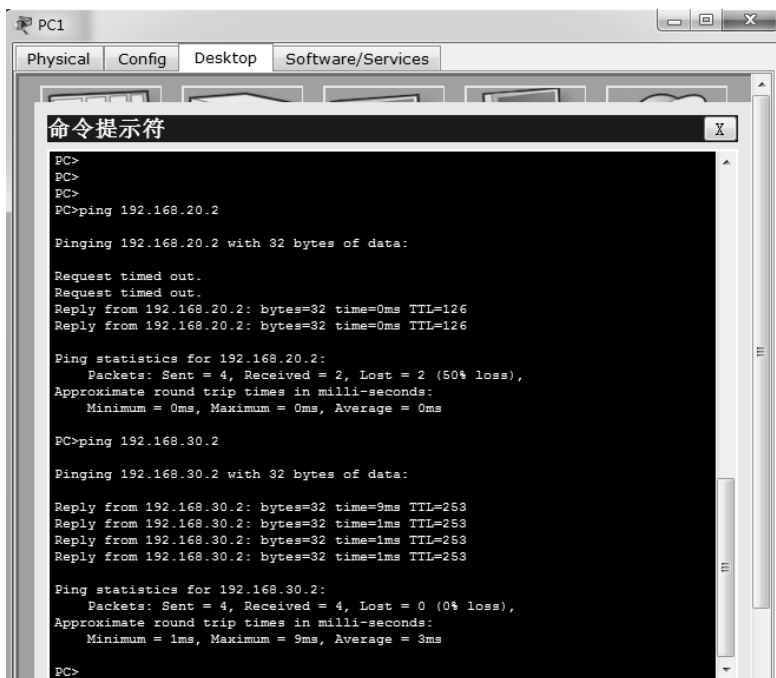


图 4-2-3 连通性测试效果图 (二)

**小贴士**

- (1) 只能宣告直连的网段。
- (2) 宣告时不附加子网掩码。
- (3) 分配的地址最好是连续的子网，以免 RIP 汇聚出现错误。

相关知识

RIP 是应用较早、使用较普遍的内部网关协议（Interior Gateway Protocol, IGP），适用于小型同类网络的一个自治系统（Autonomous System, AS）内的路由信息的传递。RIP 的管理距离为 120。RIP 是基于距离矢量算法的。它使用“跳数”，即 metric 来衡量到达目的地址的路由距离，取值为 1~15，数值 16 表示无穷大。RIP 进程使用 UDP 的 520 端口来发送和接收 RIP 分组。RIP 分组每隔 30s 以广播的形式发送一次，为了防止出现“广播风暴”，其后续的分组将做随机延时后再发送。在 RIP 中，如果一个路由在 180s 内未被刷新，则相应的距离就被设定成无穷大，并从路由表中删除该表项。

使用距离矢量路由协议的路由器并不了解到达目的网络的整条路径。距离矢量路由协议将路由器作为通往最终目的地的路径上的路标。路由器唯一了解的远程网络信息就是到达该网络的距离（即度量）以及可通过哪条路径或哪个接口到达该网络。距离矢量路由协议并不了解确切的网络拓扑图。

有两个距离矢量 IPv4 的 IGP，即 RIPv1，第一代传统协议；RIPv2，简单距离矢量路由协议。

RIPv1 被提出的较早，其中有许多缺陷。为了改善 RIPv1 的不足，在 RFC 1388 中提出了改进的 RIPv2，并在 RFC 1723 和 RFC 2453 中进行了修订。RIPv1 和 RIPv2 的区别如表 4-2-2 所示。

表 4-2-2 RIPv1 和 RIPv2 的区别

RIP v1	RIP v2
有类路由协议	无类路由协议
不能支持 VLSM 和 CIDR	可以支持 VLSM 和 CIDR
没有认证的功能	可以支持认证，并且有明文和 MD5 两种认证
手工汇总	可以在关闭自动汇总的前提下，进行手工汇总
广播更新 255.255.255.255	组播更新 224.0.0.9

在路由器上实现 RIPv1 动态路由协议的配置命令如下。

```
Router#
Router#conf t
Router(config)#router rip           ! 启动 RIP 进程
Router(config-router)#network 网段  ! 宣告相邻网段
Router(config-router)#
```

知识拓展

RIP v2 动态路由协议的实现：RIPv2 定义了一套有效的改进方案，RIPv2 支持子网路由选择，支持 CIDR，支持组播，并提供了验证机制。

配置 RIPv2 动态路由，拓扑结构如图 4-2-4 所示。

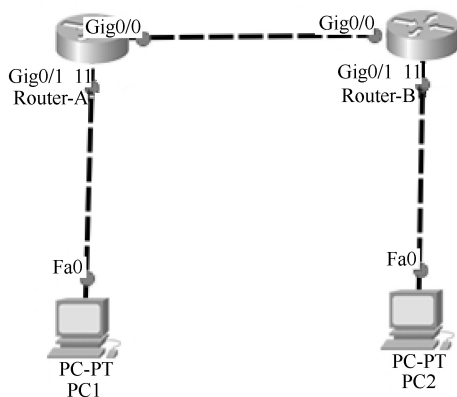


图 4-2-4 利用 RIPv2 实现网络的连通

网络参数设置如表 4-2-3 所示。

表 4-2-3 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Router-A	G0/0	172.16.2.1	255.255.255.0	无
	G0/1	172.16.1.1	255.255.255.0	无
Router-B	G0/0	172.16.2.2	255.255.255.0	无
	G0/1	172.16.3.1	255.255.255.0	无
PC1		172.16.1.2	255.255.255.0	172.16.1.1
PC2		172.16.3.2	255.255.255.0	172.16.3.1

步骤实现

步骤 1：按照图 4-2-4 连接网络拓扑结构。

步骤 2：按照表 4-2-3 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置 Router-A 的名称及其接口 IP 地址。

```

Router>en
Router#conf t
Router(config)#host Router-A
Router-A(config)#int g0/0
Router-A(config-if)#ip add 172.16.2.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int g0/1
Router-A(config-if)#ip add 172.16.1.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#^Z
Router-A#
  
```

步骤 4：配置 Router-B 的名称及其接口 IP 地址。

```

Router>en
Router#conf t
Router(config)#host Router-B
Router-B(config)#int g0/0
Router-B(config-if)#ip add 172.16.2.2 255.255.255.0
  
```



```
Router-B(config-if)#no shut
Router-B(config-if)#int g0/1
Router-B(config-if)#ip add 172.16.3.1 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#^Z
Router-B#
```

步骤 5：查看 Router-A 的接口配置情况。

```
Router-A#show ip int brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 172.16.2.1      YES manual up              up
GigabitEthernet0/1 172.16.1.1      YES manual up              up
GigabitEthernet0/2 unassigned      YES unset  administratively down down
GigabitEthernet0/2 unassigned      YES unset  administratively down down
Vlan1              unassigned      YES unset  administratively down down
Router-A#
```

步骤 6：查看 Router-B 的接口配置情况。

```
Router-B#show ip int brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 172.16.2.2      YES manual up              up
GigabitEthernet0/1 172.16.3.1      YES manual up              up
GigabitEthernet0/2 unassigned      YES unset  administratively down down
GigabitEthernet0/2 unassigned      YES unset  administratively down down
Vlan1              unassigned      YES unset  administratively down down
Router-B#
```

步骤 7：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.16.1.0/24 is directly connected, GigabitEthernet0/1
L 172.16.1.1/32 is directly connected, GigabitEthernet0/1
C 172.16.2.0/24 is directly connected, GigabitEthernet0/0
L 172.16.2.1/32 is directly connected, GigabitEthernet0/0
Router-A#
```

步骤 8：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```

Gateway of last resort is not set

```

172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C 172.16.2.0/24 is directly connected, GigabitEthernet0/0
L 172.16.2.2/32 is directly connected, GigabitEthernet0/0
C 172.16.3.0/24 is directly connected, GigabitEthernet0/1
L 172.16.3.1/32 is directly connected, GigabitEthernet0/1
Router-B#

```

步骤 9: 配置路由协议前, 使用 ping 命令测试网络的连通性。

(1) 在 PC 1 上 ping PC 2 的 IP 地址 172.16.3.2, 网络未连通, 如图 4-2-5 所示。

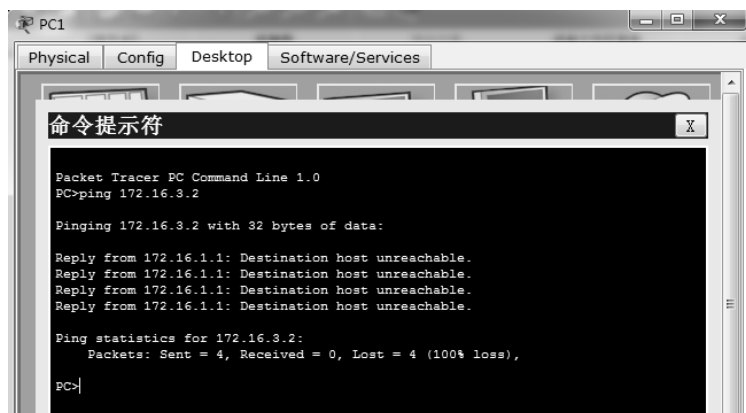


图 4-2-5 连通性测试效果图 (一)

(2) 在 PC 2 上 ping PC 1 的 IP 地址 172.16.1.2, 网络未连通, 如图 4-2-6 所示。

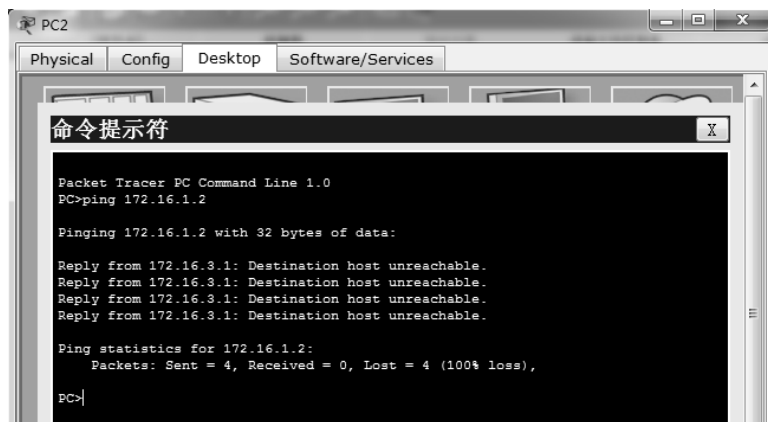


图 4-2-6 连通性测试效果图 (二)



步骤 10: 在 Router-A 上配置 RIPv2 路由协议。

```
Router-A#conf t
Router-A(config)#router rip
Router-A(config-router)#version 2
Router-A(config-router)#no auto-summary
Router-A(config-router)#network 172.16.1.1
Router-A(config-router)#network 172.16.2.1
Router-A(config-router)#
```

步骤 11: 在 Router-B 上配置 RIPv2 路由协议。

```
Router-B#conf t
Router-B(config)#router rip
Router-B(config-router)#version 2
Router-B(config-router)#no auto-summary
Router-B(config-router)#network 172.16.2.0
Router-B(config-router)#network 172.16.3.0
Router-B(config-router)#
```

步骤 12: 查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C 172.16.1.0/24 is directly connected, GigabitEthernet0/1
L 172.16.1.1/32 is directly connected, GigabitEthernet0/1
C 172.16.2.0/24 is directly connected, GigabitEthernet0/0
L 172.16.2.1/32 is directly connected, GigabitEthernet0/0
R 172.16.3.0/24 [120/1] via 172.16.2.2, 00:00:10, GigabitEthernet0/0
Router-A#
```

步骤 13: 查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
R 172.16.1.0/24 [120/1] via 172.16.2.1, 00:00:06, GigabitEthernet0/0
C 172.16.2.0/24 is directly connected, GigabitEthernet0/0
L 172.16.2.2/32 is directly connected, GigabitEthernet0/0
C 172.16.3.0/24 is directly connected, GigabitEthernet0/1
L 172.16.3.1/32 is directly connected, GigabitEthernet0/1
Router-B#
```

步骤 14: 检验现在配置的路由器仅发送和接收 RIPv2 的信息。

```
Router-A#show ip protocols
Routing Protocol is "rip"

Sending updates every 30 seconds, next due in 25 seconds
Invalid after 180 seconds, hold down 180, flushed after 240
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Redistributing: rip

Default version control: send version 2, receive 2
Interface Send Recv Triggered RIP Key-chain
GigabitEthernet0/0 2 2
GigabitEthernet0/1 2 2

Automatic network summarization is not in effect
Maximum path: 4
Routing for Networks:
172.16.0.0

Passive Interface(s):
Routing Information Sources:
Gateway Distance Last Update
172.16.2.2 120 00:00:03
Distance: (default is 120)
Router-A#
```



小贴士

注意使用 `show ip protocols` 命令时如何检验现在配置的路由器仅发送和接收 RIPv2 的信息。现在, RIP 进程在所有更新中包含子网掩码, 所以 RIPv2 是一种无类路由协议。

步骤 15: 配置路由协议后, 验证网络的连通性。

(1) 在 PC 1 上 ping PC 2 的 IP 地址 172.16.3.2, 网络已连通, 如图 4-2-7 所示。

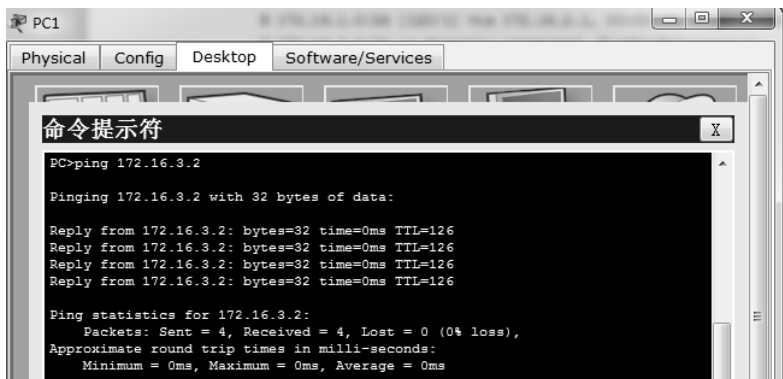


图 4-2-7 连通性测试效果图（三）

(2) 在 PC 2 上 ping PC 1 的 IP 地址 172.16.1.2，网络已连通，如图 4-2-8 所示。

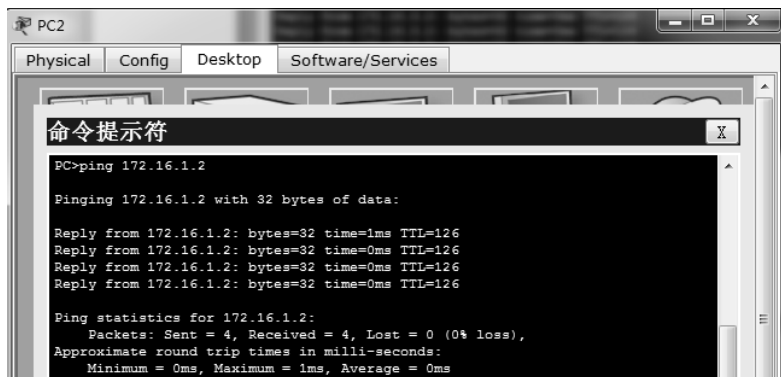


图 4-2-8 连通性测试效果图（四）



小贴士

如果不使用 RIPv2 路由协议，将导致计算机之间在使用 ping 命令测试连通性的时候丢包。

RIPv2 的命令格式如下。

```
Router#conf t
Router(config)#router rip           ! 启动 RIP 进程
Router(config-router)#version 2     ! 开启版本 2
Router(config-router)#no auto-summary ! 关闭自动汇总
Router(config-router)#network 网段  ! 宣告相邻网段
Router(config-router)#
```

学习小结

本任务介绍了网络设备之间如何实现 RIP 路由，需要注意的是，RIP 有两个版本，即 RIPv1 和 RIPv2，no auto-summary 功能只支持 RIPv2；路由器只宣告自己的直连网段，实现动态更新路由。

任务 2 EIGRP 动态路由配置

学习情境

海成公司由于规模的不断扩大，路由器已经达到了一定数量。该公司的网络管理员发现公司的所有设备都是思科公司生产的，出于网络性能的考虑，网络管理员决定在公司的路由

器之间使用思科公司私有的动态增强型内部网关路由协议（Enhanced Gateway Routing Protocol, EIGRP），实现网络的互连。

情境分析

由于公司的网络设备都是思科公司生产的，这样使用其私有的路由协议，能很大程度地提高网络的性能，所以网路管理员决定使用的动态 EIGRP 是正确的。

所需设备：

- （1）Cisco 2911 路由器 2 台。
- （2）PC 2 台。
- （3）交叉线 3 条。
- （4）Console 线 1 条。

任务拓扑结构如图 4-2-9 所示。

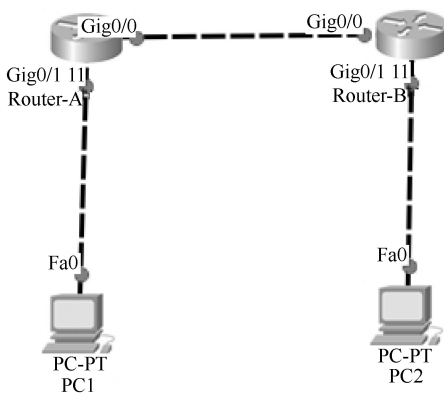


图 4-2-9 EIGRP 路由拓扑图

网络参数设置如表 4-2-4 所示。

表 4-2-4 网络参数设置

设 备	端口	IP 地址	子网掩码	网关
Router-A	G0/0	192.168.1.1	255.255.255.0	无
	G0/1	192.168.10.1	255.255.255.0	无
Router-B	G0/0	192.168.1.2	255.255.255.0	无
	G0/1	192.168.20.1	255.255.255.0	无
PC 1		192.168.10.2	255.255.255.0	192.168.10.1
PC 2		192.168.20.2	255.255.255.0	192.168.20.1

步骤实现

步骤 1：按照图 4-2-9 连接网络拓扑结构。

步骤 2：按照表 4-2-4 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置 Router-A 的名称及其接口 IP 地址。

```
Router>en
Router#conf t
Router(config)#host Router-A
Router-A(config)#int g0/0
Router-A(config-if)#ip add 192.168.1.1 255.255.255.0
```



```
Router-A(config-if)#no shut
Router-A(config-if)#int g0/1
Router-A(config-if)#ip add 192.168.10.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#^Z
Router-A#
```

步骤 4：配置 Router-B 的名称及其接口 IP 地址。

```
Router>en
Router#conf t
Router(config)#host Router-B
Router-B(config)#int g0/0
Router-B(config-if)#ip add 192.168.1.2 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#int g0/1
Router-B(config-if)#ip add 192.168.20.1 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#^Z
Router-B#
```

步骤 5：查看 Router-A 的接口配置情况。

```
Router-A#show ip int brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 192.168.1.1     YES manual up              up
GigabitEthernet0/1 192.168.10.1    YES manual up              up
GigabitEthernet0/2 unassigned      YES unset  administratively down down
Vlan1              unassigned      YES unset  administratively down down
Router-A#
```

步骤 6：查看 Router-B 的接口配置情况。

```
Router-B#show ip int brief
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 192.168.1.2     YES manual up              up
GigabitEthernet0/1 192.168.20.1    YES manual up              up
GigabitEthernet0/2 unassigned      YES unset  administratively down down
Vlan1              unassigned      YES unset  administratively down down
Router-B#
```

步骤 7：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1
Router-A#
```

步骤 8: 查看 Router-B 的路由表。

```
Router-B#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.2/32 is directly connected, GigabitEthernet0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/1
L 192.168.20.1/32 is directly connected, GigabitEthernet0/1
Router-B#
```

步骤 9: 配置路由协议前, 使用 ping 命令测试网络的连通性。

(1) 在 PC 1 上 ping PC 2 的 IP 地址 “ping 192.168.20.2”, 网络未连通, 如图 4-2-10 所示。

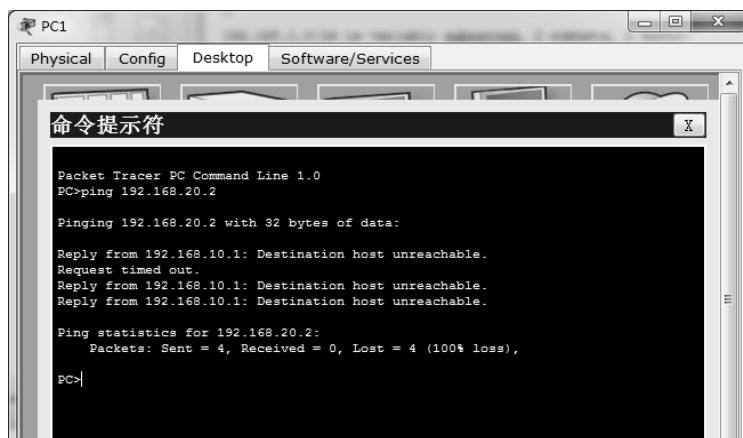


图 4-2-10 连通性测试效果图 (一)



(2) 在 PC 2 上 ping PC 1 的 IP 地址 “ping 192.168.10.2”，网络未连通，如图 4-2-11 所示。

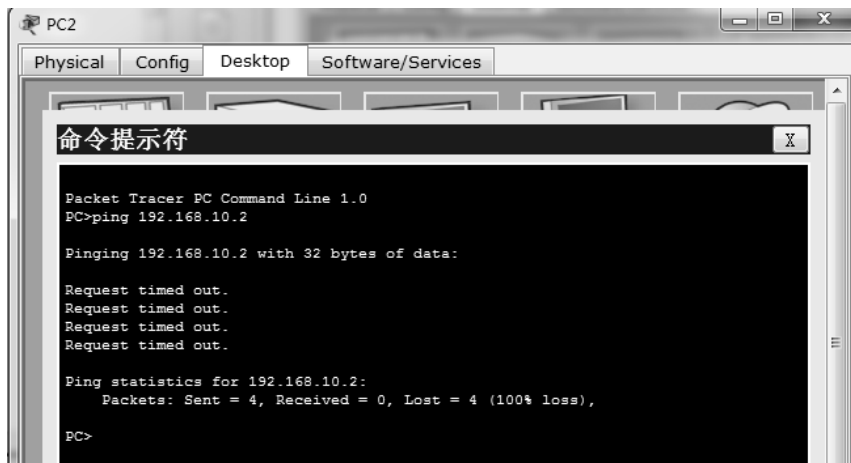


图 4-2-11 连通性测试效果图（二）

步骤 10：在 Router-A 上配置动态 EIGRP。

```
Router-A(config)#router eigrp 100
Router-A(config-router)#network 192.168.1.0
Router-A(config-router)#network 192.168.10.0
Router-A(config-router)#
```

步骤 11：在 Router-B 上配置动态 EIGRP。

```
Router(config)#router eigrp 100
Router(config-router)#network 192.168.1.0
Router(config-router)#network 192.168.20.0
Router(config-router)#
```

步骤 12：查看 Router-A 的路由表。

```
Router-A#show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C 192.168.10.0/24 is directly connected, GigabitEthernet0/1
L 192.168.10.1/32 is directly connected, GigabitEthernet0/1
D 192.168.20.0/24 [90/3072] via 192.168.1.2, 00:00:59, GigabitEthernet0/0
Router-A#
```

步骤 13: 查看 Router-B 的路由表。

```
Rotuer-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.2/32 is directly connected, GigabitEthernet0/0
D 192.168.10.0/24 [90/3072] via 192.168.1.1, 00:01:31, GigabitEthernet0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/1
L 192.168.20.1/32 is directly connected, GigabitEthernet0/1
Rotuer-B#
```

步骤 14: 配置路由协议后, 使用 ping 命令验证网络的连通性。

(1) 在 PC 1 上 ping PC 2 的 IP 地址 192.168.20.2, 网络已连通, 如图 4-2-12 所示。

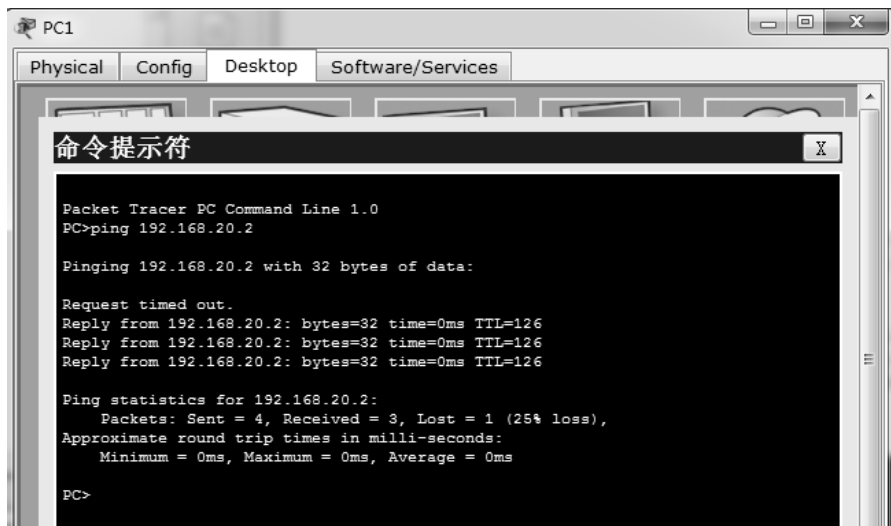


图 4-2-12 连通性测试效果图 (一)



(2) 在 PC 2 上 ping PC 1 的 IP 地址 192.168.10.2, 网络已连通, 如图 4-2-13 所示。

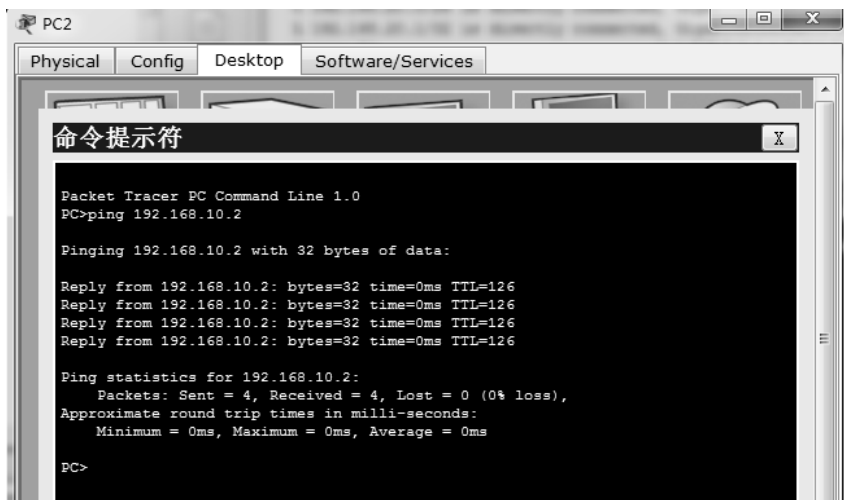


图 4-2-13 连通性测试效果图（二）

相关知识

EIGRP 是 Cisco Systems 开发的高级距离矢量路由协议。顾名思义, EIGRP 是另一种思科路由协议 IGRP 的增强版。IGRP 是较早的有类距离矢量路由协议, 自 IOS 12.3 后已被淘汰。

EIGRP 具备链路状态路由协议的某些功能, 是一种距离矢量路由协议。EIGRP 适用于不同的拓扑结构和介质。在设计合理的网络中, EIGRP 能够加以扩展从而包含多个拓扑, 并能够以最小的网络流量达到极快的融合速度。

EIGRP 最初发布于 1992 年, 是只适用于思科设备的专有协议。2013 年, 思科公司以开放标准形式向 IETF 发布了 EIGRP 的基本功能作为信息性 RFC。这意味着其他网络供应商现在可以在其设备上实施 EIGRP, 从而与运行 EIGRP 的思科路由器和非思科路由器互操作。然而, EIGRP 高级功能不会向 IETF 发布, 如部署动态多点虚拟专用网络 (DMVPN) 所需的 EIGRP 末节。作为信息性 RFC, 思科公司将继续保持对 EIGRP 的控制。

EIGRP 兼具链路状态路由协议和距离矢量路由协议的功能。但 EIGRP 依然基于距离矢量路由协议的核心原理, 其中关于其他网络的信息是从直连的邻居获得的。

EIGRP 路由协议的相关命令如下。

```
Router(config)#router eigrp autonomous-system      !指定使用 EIGRP 协议
Router(config-router)# network network              !指定与该路由器相连的网络
Router(config-router)#
```

注意: autonomous-system 的取值为 1~65536 的任意值, 并非实际意义上的 autonomous-system, 但运行 EIGRP 的路由器要想交换路由、更新信息, 则其 autonomous-system 需要相同。

知识拓展

三层交换机实现 EIGRP 动态路由协议: 配置 EIGRP 动态路由, 如图 4-2-14 所示。

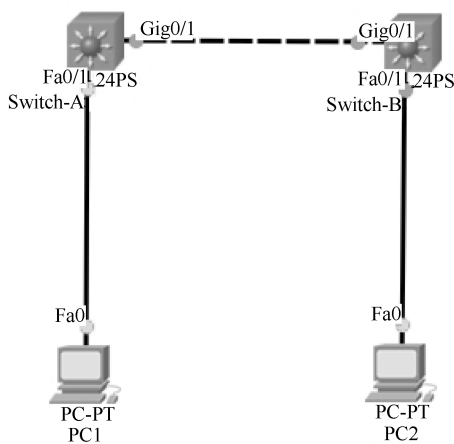


图 4-2-14 默认路由拓扑图

网络参数设置如表 4-2-5 所示。

表 4-2-5 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Switch-A	G0/1	192.168.1.1	255.255.255.0	无
	Fa0/1	192.168.10.1	255.255.255.0	无
Switch-B	G0/1	192.168.1.2	255.255.255.0	无
	Fa0/1	192.168.20.1	255.255.255.0	无
PC1		192.168.10.2	255.255.255.0	192.168.10.1
PC2		192.168.20.2	255.255.255.0	192.168.20.1

步骤实现

- 步骤 1：按照图 4-2-14 连接网络拓扑结构。
- 步骤 2：按照表 4-2-5 配置计算机的 IP 地址、子网掩码和网关。
- 步骤 3：配置 Switch-A 的名称及其接口 IP 地址。

```
Switch>
Switch>enable
Switch#conf t
Switch(config)#host Switch-A
Switch-A(config)#ip routing
Switch-A(config)#int g0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.1.1 255.255.255.0
Switch-A(config-if)#int fa0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.10.1 255.255.255.0
Switch-A(config-if)#
```

- 步骤 4：配置 Switch-B 的名称及其接口 IP 地址。

```
Switch>enable
Switch#conf t
```



```
Switch(config)#host Switch-B
Switch-B(config)#ip routing
Switch-B(config)#int g0/1
Switch-B(config-if)#no switchport
Switch-B(config-if)#ip add 192.168.1.2 255.255.255.0
Switch-B(config-if)#no shut
Switch-B(config-if)#int fa0/1
Switch-B(config-if)#no switchport
Switch-B(config-if)#ip add 192.168.20.1 255.255.255.0
Switch-B(config-if)#no shut
Switch-B(config-if)#
```

步骤 5：查看 Switch-A 的路由表。

```
Switch-A# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
C 192.168.10.0/24 is directly connected, FastEthernet0/1
Switch-A#
```

步骤 6：查看 Switch-B 的路由表。

```
Switch-B#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
C 192.168.20.0/24 is directly connected, FastEthernet0/1
Switch-B#
```

步骤 7：配置路由协议前，使用 ping 命令测试网络的连通性。

(1) 在 PC1 上 ping PC 2 的 IP 地址 192.168.20.2，网络未连通，如图 4-2-15 所示。

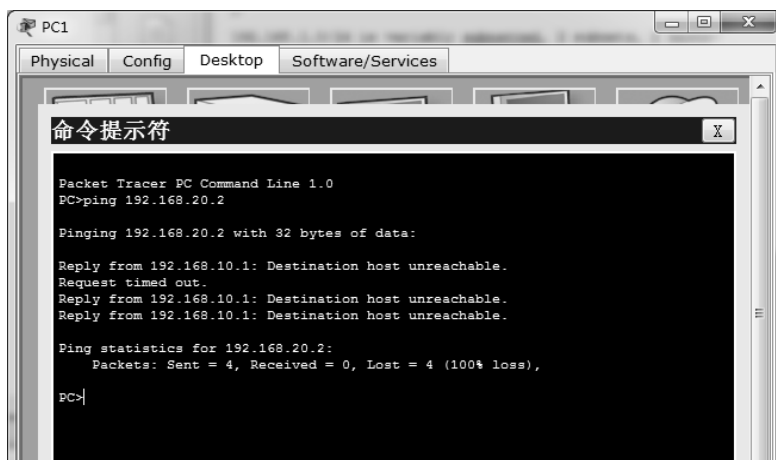


图 4-2-15 连通性测试效果图（一）

(2) 在 PC 2 上 ping PC 1 的 IP 地址 192.168.10.2，网络未连通，如图 4-2-16 所示。

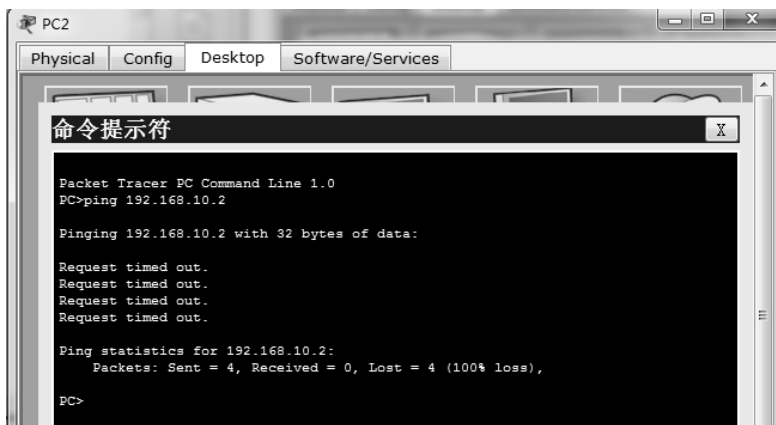


图 4-2-16 连通性测试效果图（二）

步骤 8：在 Switch-A 上配置动态 EIGRP。

```
Switch-A#
Switch-A#conf t
Switch-A(config)#router eigrp 100
Switch-A(config-router)#network 192.168.1.0
Switch-A(config-router)#network 192.168.10.0
Switch-A(config-router)#
```

步骤 9：在 Switch-B 上配置动态 EIGRP。

```
Switch-B#
Switch-B#conf t
Switch-B(config)#router eigrp 100
Switch-B(config-router)#network 192.168.1.0
Switch-B(config-router)#network 192.168.20.0
Switch-B(config-router)#
```

步骤 10：查看 Switch-A 的路由表。

```
Switch-A#show ip route
```



```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
C 192.168.10.0/24 is directly connected, FastEthernet0/1
D 192.168.20.0/24 [90/28416] via 192.168.1.2, 00:01:16, GigabitEthernet0/1
Switch-A#
```

步骤 11: 查看 Switch-B 的路由表。

```
Switch-B#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is not set

```
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
D 192.168.10.0/24 [90/28416] via 192.168.1.1, 00:03:13, GigabitEthernet0/1
C 192.168.20.0/24 is directly connected, FastEthernet0/1
Switch-B#
```

步骤 12: 配置路由协议后，使用 ping 命令验证网络的连通性。

(1) 在 PC 1 上 ping PC 2 的 IP 地址 192.168.20.2，网络已连通，如图 4-2-17 所示。

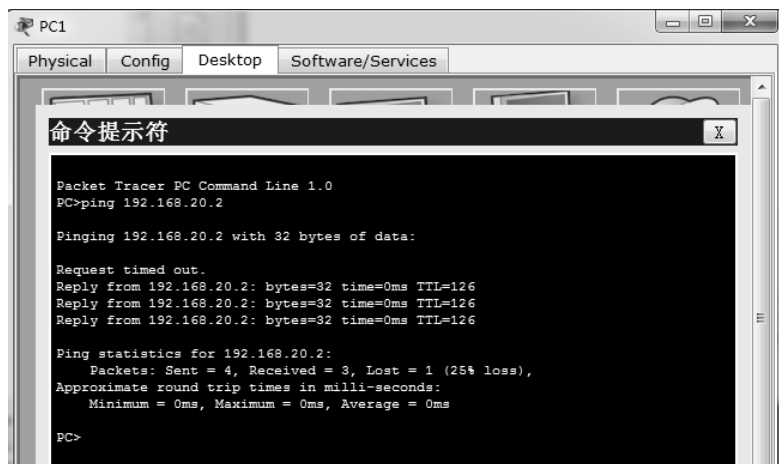


图 4-2-17 连通性测试效果图（三）

(2) 在 PC 2 上 ping PC 1 的 IP 地址 192.168.10.2, 网络已连通, 如图 4-2-18 所示。

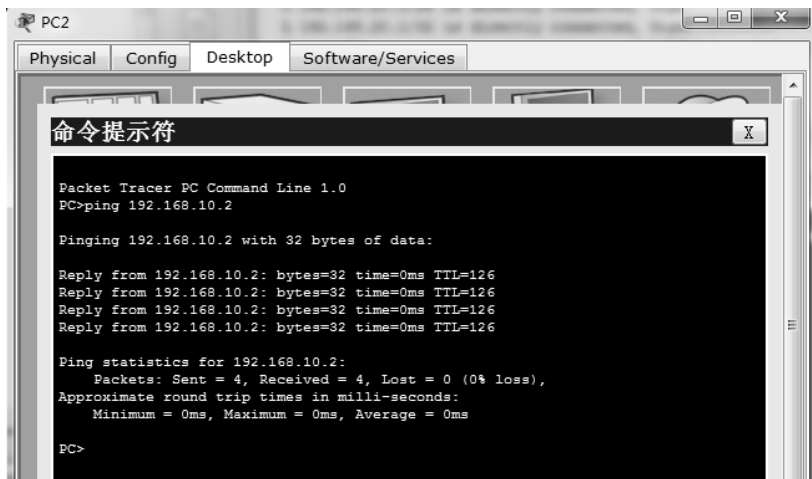


图 4-2-18 连通性测试效果图 (四)

学习小结

本任务介绍了路由器之间如何实现动态 EIGRP, 使用 EIGRP 路由协议时, 每个路由器的进程号需要一致。需要注意的是, EIGRP 是思科公司的私有协议, 其他厂商是没有此协议的。

任务 3 OSPF 动态路由配置

开放式最短路径优先 (Open Shortest Path First, OSPF) 协议是目前网络中应用最广泛的动态路由协议之一。它也属于内部网关路由协议, 能够适应各种规模的网络环境, 是典型的链路状态路由协议。

学习情境

海成公司的规模越来越大, 路由器的数量也逐渐增多, 已经达到了 8 台。该公司的网络管理员发现原有的 RIP 路由协议已不再适合现有公司的应用, 因此, 决定在公司的路由器之间使用动态的 OSPF 路由协议, 实现网络的互连。

情境分析

由于公司的网络规模越来越大, 网络管理员发现使用 OSPF 路由协议再适合不过, 因为 OSPF 路由协议可以实现快速收敛, 并且出现环路的可能性不大, 适合中大型企业网络的使用。

所需设备:

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco 3560-24PS 交换机 1 台。
- (3) PC 3 台。
- (4) 交叉线 2 条。
- (5) 直通线 2 条。
- (6) DCE 串口和 DTE 串口线 1 条。
- (7) Console 线 1 条。

任务拓扑结构如图 4-2-19 所示。

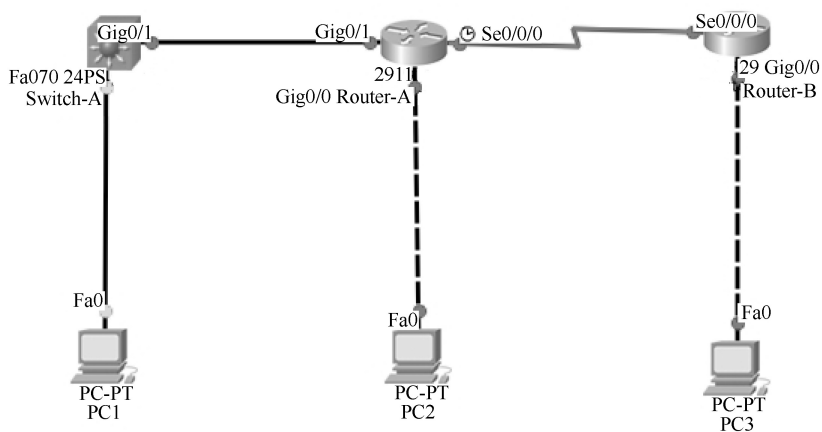


图 4-2-19 配置 OSPF 协议单区域拓扑

网络参数设置如表 4-2-6 所示。

表 4-2-6 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Switch-A	G0/1	192.168.1.1	255.255.255.0	无
	F0/1	192.168.10.1	255.255.255.0	无
Router-A	G0/1	192.168.1.2	255.255.255.0	无
	G0/0	192.168.20.1	255.255.255.0	无
	S0/0/0	192.168.2.1	255.255.255.0	无
Router-B	S0/0/0	192.168.2.2	255.255.255.0	无
	G0/0	192.168.30.1	255.255.255.0	无
PC 1		192.168.10.2	255.255.255.0	192.168.10.1
PC 2		192.168.20.2	255.255.255.0	192.168.20.1
PC 3		192.168.30.2	255.255.255.0	192.168.30.1

步骤实现

步骤 1：按照图 4-2-19 连接网络拓扑结构。

步骤 2：按照表 4-2-6 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置 Switch-A 的名称及其接口 IP 地址。

```
Switch>
Switch>enable
Switch#conf t
Switch(config)#host Switch-A
Switch-A(config)#ip routing
Switch-A(config)#int fa0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.10.1 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config-if)#int g0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.1.1 255.255.255.0
```

```
Switch-A(config-if)#no shut
Switch-A(config-if)#exit
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router>enable
Router#conf t
Router(config)#host Router-A
Router-A(config)#int g0/1
Router-A(config-if)#ip add 192.168.1.2 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int g0/0
Router-A(config-if)#ip add 192.168.20.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int s0/0/0
Router-A(config-if)#clock rate 64000
Router-A(config-if)#ip add 192.168.2.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#
```

步骤 5：配置 Router-B 的名称及其接口 IP 地址。

```
Router>en
Router#conf t
Router(config)#host Router-B
Router-B(config)#int g0/0
Router-B(config-if)#ip add 192.168.30.1 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#int s0/0/0
Router-B(config-if)#ip add 192.168.2.2 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#
```

步骤 6：查看 Switch-A 的接口配置情况。

```
Switch-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	192.168.10.1	YES	manual	up	up
GigabitEthernet0/1	192.168.1.1	YES	manual	up	up

步骤 7：查看 Router-A 的接口配置情况。

```
Router-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.20.1	YES	manual	up	up
GigabitEthernet0/1	192.168.1.2	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Serial0/0/0	192.168.2.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router-A#
```




步骤 8：查看 Router-B 的接口配置情况。

```
Router-B#show ip int brief
Interface                IP-Address      OK? Method Status      Protocol
GigabitEthernet0/0       192.168.30.2    YES manual  up           up
GigabitEthernet0/1       unassigned      YES unset   administratively down down
GigabitEthernet0/2       unassigned      YES unset   administratively down down
Serial10/0/0             192.168.2.2     YES manual  up           up
Serial10/0/1             unassigned      YES unset   administratively down down
Vlan1                    unassigned      YES unset   administratively down down
Router-B#
```

步骤 9：查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.2/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial10/0/0
L 192.168.2.1/32 is directly connected, Serial10/0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
Router-A#
```

步骤 10：查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.2/32 is directly connected, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0
L 192.168.30.2/32 is directly connected, GigabitEthernet0/0
Router-B#
```

步骤 11: 查看 Switch-A 的路由表。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
C 192.168.10.0/24 is directly connected, FastEthernet0/1
Switch-A#
```

步骤 12: 配置路由协议前, 使用 ping 命令测试网络的连通性。在 PC 1 上 ping PC 2 和 PC 3 的 IP 地址, 网络未连通, 如图 4-2-20 所示。

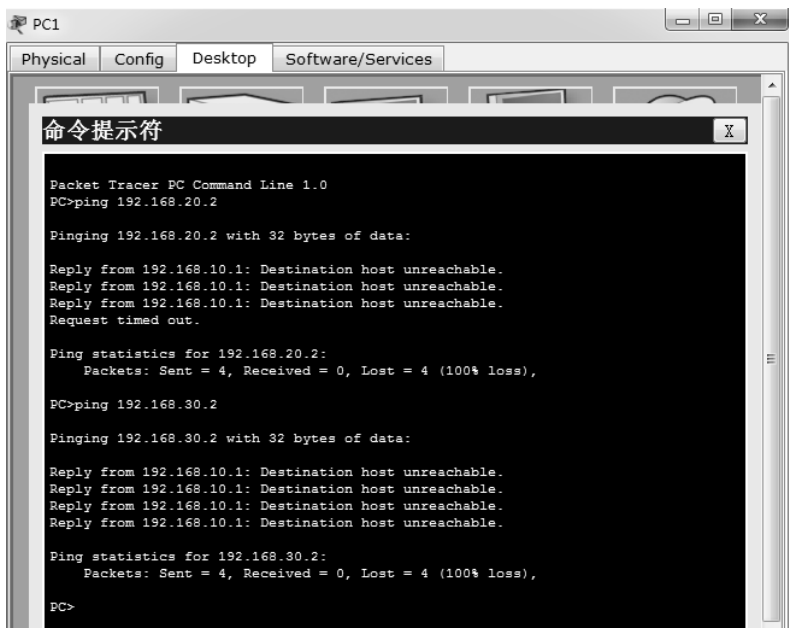


图 4-2-20 连通性测试效果图 (未连通)



步骤 13：在 Switch-A 上配置动态单区域 OSPF 协议。

```
Switch-A>en
Switch-A#conf t
Switch-A(config)#router ospf 1
Switch-A(config-router)#network 192.168.10.0 0.0.0.255 area 0
Switch-A(config-router)#network 192.168.1.0 0.0.0.255 area 0
Switch-A(config-router)#
```

步骤 14：在 Router-A 上配置动态单区域 OSPF 协议。

```
Router-A>
Router-A>enable
Router-A#conf t
Router-A(config)#router ospf 1
Router-A(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router-A(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router-A(config-router)#network 192.168.20.0 0.0.0.255 area 0
Router-A(config-router)#
```

步骤 15：在 Router-B 上配置动态单区域 OSPF 协议。

```
Router-B#
Router-B#conf t
Router-B(config)#router ospf 1
Router-B(config-router)#network 192.168.2.0 0.0.0.255 area 0
Router-B(config-router)#network 192.168.30.0 0.0.0.255 area 0
Router-B(config-router)#
```



小贴士

在配置 OSPF 通告相应网络时要确保子网掩码的配置正确，且要说明路由器所在的区域。

步骤 16：查看 Switch-A 的路由表。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
O 192.168.2.0/24 [110/65] via 192.168.1.2, 00:00:15, GigabitEthernet0/1
C 192.168.10.0/24 is directly connected, FastEthernet0/1
O 192.168.20.0/24 [110/2] via 192.168.1.2, 00:00:15, GigabitEthernet0/1
O 192.168.30.0/24 [110/66] via 192.168.1.2, 00:00:15, GigabitEthernet0/1
Switch-A#
```

步骤 17: 查看 Router-A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.2/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
O 192.168.10.0/24 [110/2] via 192.168.1.1, 00:00:03, GigabitEthernet0/1
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
O 192.168.30.0/24 [110/65] via 192.168.2.2, 00:02:05, Serial0/0/0
Router-A#
```

步骤 18: 查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.1.0/24 [110/65] via 192.168.2.1, 00:00:27, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.2/32 is directly connected, Serial0/0/0
O 192.168.10.0/24 [110/66] via 192.168.2.1, 00:00:27, Serial0/0/0
O 192.168.20.0/24 [110/65] via 192.168.2.1, 00:02:34, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
```



```
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0
L 192.168.30.1/32 is directly connected, GigabitEthernet0/0
Router-B#
```

步骤 19：配置路由协议后，使用 ping 命令验证网络的连通性。在 PC 1 上 ping PC 2 和 PC 3 的 IP 地址，网络已连通，如图 4-2-21 所示。

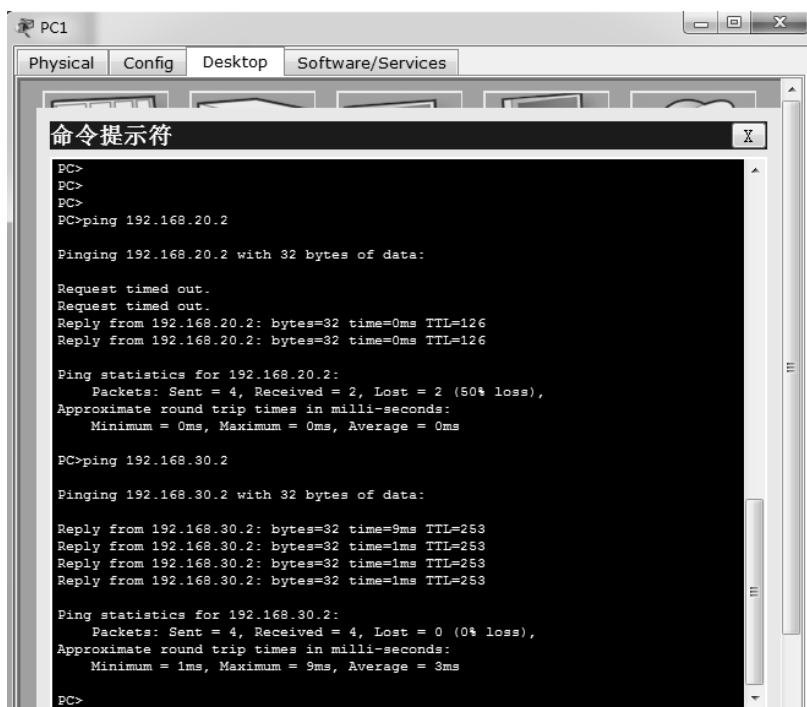


图 4-2-21 连通性测试效果图（连通）



小贴士

- (1) 每个路由器的 OSPF 进程号可以不同，一个路由器可以有多个 OSPF 进程。
- (2) OSPF 是无类路由协议，一定要加子网掩码。
- (3) 第一个区域必须是区域 0。

相关知识

OSPF 协议是一种链路状态路由协议，旨在替代距离矢量路由协议 RIP。RIP 是网络和 Internet 早期广为接受的路由协议。但是，RIP 依靠跳数作为确定最佳路由的唯一度量，很快便出现了问题。在速度各异的多条路径的大型网络中，使用跳数无法很好地扩展。OSPF 与 RIP 相比具有巨大优势，因为它既能快速收敛，又能扩展到更大型的网络。其特性如下。

- (1) 适用范围广：支持各种规模的网络，最多可支持几百台路由器。
- (2) 收敛快速：在网络的拓扑结构发生变化后立即发送更新报文，使这一变化在自治系统中同步。
- (3) 无自环：OSPF 根据收集到的链路状态用最短路径树算法计算路由，从算法本身保证了不会生成自环路由。
- (4) 区域划分管理：允许自治系统的网络被划分为区域以便于管理，区域间传送的路由

信息被进一步抽象，从而减少了占用的网络带宽。

(5) 路由分级：使用 4 类不同等级的路由，按优先顺序分别是区域内路由、区域间路由、第一类外部路由、第二类外部路由。

(6) 支持验证：支持基于接口的报文验证，以保证路由计算的安全性。

(7) 可以多播发送：在有多播发送能力的链路层上以多播地址收发报文，既达到了广播的作用，又最大程度地减少了对其他网络的干扰。

OSPF 路由协议通过向全网通告自己的路由信息，使网络中每台设备最终同步一个具有全网链路状态的数据库，然后路由器采用 SPF 算法，以自己为根，计算到达其他网络的最短路径，最终形成全网路由信息。

在大型的网络环境中，OSPF 支持区域的划分，将网络进行合理规划。划分区域时必须存在 area0（骨干区域）。其他区域和骨干区域直接相连，或通过虚链路连接。

要创建 OSPF 路由进程，在全局命令配置模式下，执行以下命令。

```
router#config
router_config#router ospf process-id      !启动 OSPF 路由进程
router_config_router_process-id#network address wildcard-mask area area-id
router_config_router_process-id#
```

(1) OSPF 路由进程 process-id 必须指定为 1~65535，多个 OSPF 进程可以在同一个路由器上配置，但最好不这样操作。多个 OSPF 进程需要多个 OSPF 数据库的副本，必须运行多个最短路径算法的副本。process-id 只在路由器内部起作用，不同路由器的 process-id 可以不同。

(2) wildcard-mask 是子网掩码的反码，网络区域 ID area-id 可以是在 0~4294967295 内的十进制数，也可以是带有 IP 地址格式的 x.x.x.x。当网络区域 ID 为 0 或 0.0.0.0 时，该区域为主干区域。不同网络区域的路由器通过主干域学习路由信息。

知识拓展

OSPF 动态路由协议多区域的实现：当大型 OSPF 区域分成较小的区域时，被称为多区域 OSPF。多区域 OSPF 在大型网络部署时很有用，能减少处理和内存开销。

例如，每当路由器收到有关拓扑结构的新信息时，如链路的添加、删除或修改，路由器必须重新运行 SPF 算法，创建新的 SPF 树并更新路由表。SPF 算法会占用很多 CPU 资源，且其耗费的计算时间取决于区域的大小。一个区域中有过多路由器会使 LSDB 更大并增加 CPU 的负载。因此，将路由器有效分区可以把一个巨大的数据库分成更小、更易管理的数据库。

多区域 OSPF 需要使用分层网络设计。主干区域是区域 0，而且所有其他区域必须连接到主干区域。采用分层路由后，各个区域之间仍然能够进行路由（区域间路由）；但许多烦琐的路由操作（如重新计算数据库）在区域内进行。

对于复杂的网络，OSPF 可使用多个区域以分层方式实施。所有区域必须连接到主干区域（区域 0）。互连各个区域的路由器称为区域边界路由器（ABR）。

利用多区域 OSPF，OSPF 可以把一个大型自治系统划分为更小的区域，以支持分层路由。

注意：拓扑更改以距离矢量格式分布到其他区域中的路由器中。换句话说，这些路由器只会更新其路由表，无需重新运行 SPF 算法。

多区域 OSPF 的分层拓扑具有以下优势。



（1）路由表减小：路由表条目减少，因为区域之间的网络地址可以总结。默认情况下不启用路由总结。

（2）链路状态更新开销减少：将处理和内存要求降到最低。

（3）SPF 计算频率降低：使拓扑变化仅影响区域内部。例如，由于 LSA 泛洪在区域边界终止，因此它使得路由更新的影响降到最小。

所需设备：

- （1）Cisco 2911 路由器 2 台。
- （2）Cisco 3560-24PS 交换机 1 台。
- （3）PC 3 台。
- （4）交叉线 2 条。
- （5）直通线 2 条。
- （6）DCE 串口和 DTE 串口线 1 条。
- （7）Console 线 1 条。

任务拓扑结构如图 4-2-22 所示。

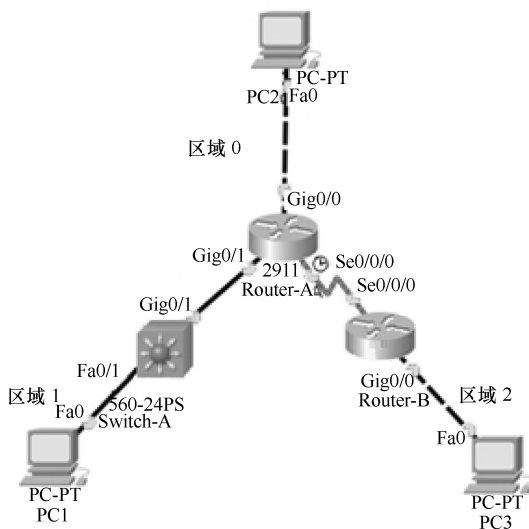


图 4-2-22 配置 OSPF 多区域

网络参数设置如表 4-2-7 所示。

表 4-2-7 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关	所 属 区 域
Switch-A	G0/1	192.168.1.1	255.255.255.0	无	0
	F0/1	192.168.10.1	255.255.255.0	无	1
Router-A	G0/1	192.168.1.2	255.255.255.0	无	0
	G0/0	192.168.20.1	255.255.255.0	无	0
	S0/0/0	192.168.2.1	255.255.255.0	无	0

(续表)

设 备	端 口	IP 地址	子网掩码	网关	所 属 区 域
Router-B	S0/0/0	192.168.2.2	255.255.255.0	无	0
	G0/0	192.168.30.1	255.255.255.0	无	2
PC 1		192.168.10.2	255.255.255.0	192.168.10.1	1
PC 2		192.168.20.2	255.255.255.0	192.168.20.1	0
PC 3		192.168.30.2	255.255.255.0	192.168.30.1	2

步骤实现

步骤 1：按照图 4-2-22 连接网络拓扑结构。

步骤 2：按照表 4-2-7 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置 Switch-A 的名称及其接口 IP 地址。

```
Switch>
Switch>enable
Switch#conf t
Switch(config)#host Switch-A
Switch-A(config)#ip routing
Switch-A(config)#int fa0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.10.1 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config-if)#int g0/1
Switch-A(config-if)#no switchport
Switch-A(config-if)#ip add 192.168.1.1 255.255.255.0
Switch-A(config-if)#no shut
Switch-A(config-if)#exit
```

步骤 4：配置 Router-A 的名称及其接口 IP 地址。

```
Router>enable
Router#conf t
Router(config)#host Router-A
Router-A(config)#int g0/1
Router-A(config-if)#ip add 192.168.1.2 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int g0/0
Router-A(config-if)#ip add 192.168.20.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#int s0/0/0
Router-A(config-if)#clock rate 64000
Router-A(config-if)#ip add 192.168.2.1 255.255.255.0
Router-A(config-if)#no shut
Router-A(config-if)#
```

步骤 5：配置 Router-B 的名称及其接口 IP 地址。

```
Router>en
Router#conf t
```




```
Router(config)#host Router-B
Router-B(config)#int g0/0
Router-B(config-if)#ip add 192.168.30.1 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#int s0/0/0
Router-B(config-if)#ip add 192.168.2.2 255.255.255.0
Router-B(config-if)#no shut
Router-B(config-if)#
```

步骤 6：查看 Switch-A 的接口配置情况。

```
Switch-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	192.168.10.1	YES	manual	up	up
GigabitEthernet0/1	192.168.1.1	YES	manual	up	up

步骤 7：查看 Router-A 的接口配置情况。

```
Router-A#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.20.1	YES	manual	up	up
GigabitEthernet0/1	192.168.1.2	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Serial0/0/0	192.168.2.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router-A#
```

步骤 8：查看 Router-B 的接口配置情况。

```
Router-B#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	192.168.30.2	YES	manual	up	up
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
Serial0/0/0	192.168.2.2	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router-B#
```

步骤 9：查看 Router-A 的路由表。

```
Router-A#show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```
Gateway of last resort is not set
```

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.2/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
Router-A#
```

步骤 10: 查看 Router-B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.2/32 is directly connected, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0
L 192.168.30.2/32 is directly connected, GigabitEthernet0/0
Router-B#
```

步骤 11: 查看 Switch-A 的路由表。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
```



```
C 192.168.10.0/24 is directly connected, FastEthernet0/1
Switch-A#
```

步骤 12：配置路由协议前，使用 ping 命令测试网络的连通性。在 PC 1 上 ping PC 2 和 PC 3 的 IP 地址，网络未连通，如图 4-2-23 所示。

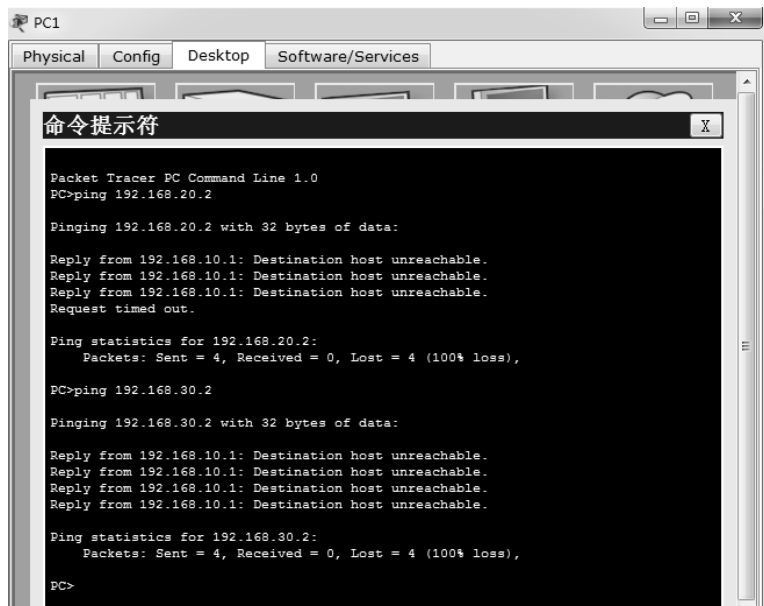


图 4-2-23 连通性测试效果图（未连通）

步骤 13：在 Switch-A 上配置动态多区域 OSPF 路由协议。

```
Switch-A>en
Switch-A#conf t
Switch-A(config)#router ospf 1
Switch-A(config-router)#network 192.168.10.0 0.0.0.255 area 0
Switch-A(config-router)#network 192.168.1.0 0.0.0.255 area 0
Switch-A(config-router)#
```

步骤 14：在 Router-A 上配置动态多区域 OSPF 路由协议。

```
Router-A>
Router-A>enable
Router-A#conf t
Router-A(config)#router ospf 1
Router-A(config-router)#network 192.168.1.0 0.0.0.255 area 0
Router-A(config-router)#network 192.168.2.0 0.0.0.255 area 2
Router-A(config-router)#network 192.168.20.0 0.0.0.255 area 1
Router-A(config-router)#
```

步骤 15：在 Router-B 上配置动态多区域 OSPF 路由协议。

```
Router-B#
Router-B#conf t
Router-B(config)#router ospf 1
Router-B(config-router)#network 192.168.2.0 0.0.0.255 area 2
Router-B(config-router)#network 192.168.30.0 0.0.0.255 area 2
```

```
Router-B(config-router)#
```



小贴士

在配置 OSPF 通告相应网络时要确保子网掩码的反码配置正确，且要说明路由器所在的区域。

步骤 16: 查看 Switch-A 的路由表。

```
Switch-A#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
O 192.168.2.0/24 [110/65] via 192.168.1.2, 00:01:21, GigabitEthernet0/1
C 192.168.10.0/24 is directly connected, FastEthernet0/1
O 192.168.20.0/24 [110/2] via 192.168.1.2, 00:01:21, GigabitEthernet0/1
O IA 192.168.30.0/24 [110/66] via 192.168.1.2, 00:00:26, GigabitEthernet0/1
Switch-A#
```

步骤 17: 查看 Router-A 的路由表。

```
Router-A# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.2/32 is directly connected, GigabitEthernet0/1
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.1/32 is directly connected, Serial0/0/0
O IA 192.168.10.0/24 [110/2] via 192.168.1.1, 00:01:48, GigabitEthernet0/1
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
O IA 192.168.30.0/24 [110/65] via 192.168.2.2, 00:00:32, Serial0/0/0
Router-A#
```



步骤 18: 查看 Router-B 的路由表。

```
Router-B# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is not set

O 192.168.1.0/24 [110/65] via 192.168.2.1, 00:00:15, Serial0/0/0
192.168.2.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.2.0/24 is directly connected, Serial0/0/0
L 192.168.2.2/32 is directly connected, Serial0/0/0
O 192.168.10.0/24 [110/66] via 192.168.2.1, 00:00:15, Serial0/0/0
O 192.168.20.0/24 [110/65] via 192.168.2.1, 00:00:15, Serial0/0/0
192.168.30.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.30.0/24 is directly connected, GigabitEthernet0/0
L 192.168.30.1/32 is directly connected, GigabitEthernet0/0
Router-B#
```

步骤 19: 配置路由协议后, 使用 ping 命令验证网络的连通性。在 PC 1 上 ping PC 2 和 PC 3 的 IP 地址, 网络已连通, 如图 4-2-24 所示。

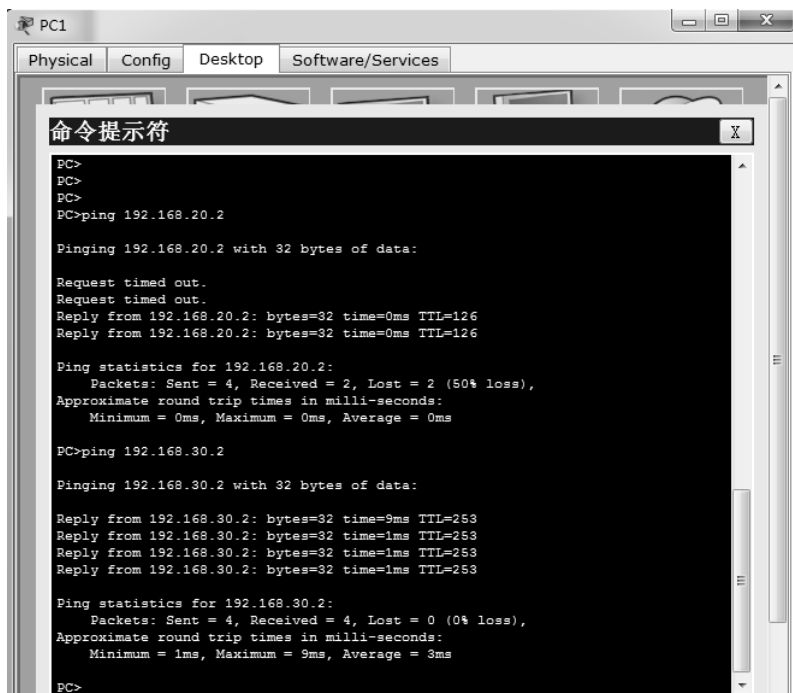


图 4-2-24 连通性测试效果图（连通）



小贴士

在配置 OSPF 多区域时，骨干区域（area 0）只有一个，且要为每个路由器指定所在的区域。

学习小结

本任务介绍了路由器之间如何实现动态路由 OSPF 协议，使用 OSPF 路由协议在宣告直连网段时，需要使用该网段的子网掩码，而且必须指明所属的区域。

项目考核

(1) 任务：配置 RIP。

某公司规模很小，只有一家上海分公司，经理决定组建一个网络实现公司总部和分公司的通信，公司网络管理员经过分析，决定使用静态路由协议，如图 4-2-25 所示。

(1) 使用静态路由协议实现全网互通。

(2) 将静态路由清除，用 RIPv2 实现全网互通，注意三层交换机上的配置。

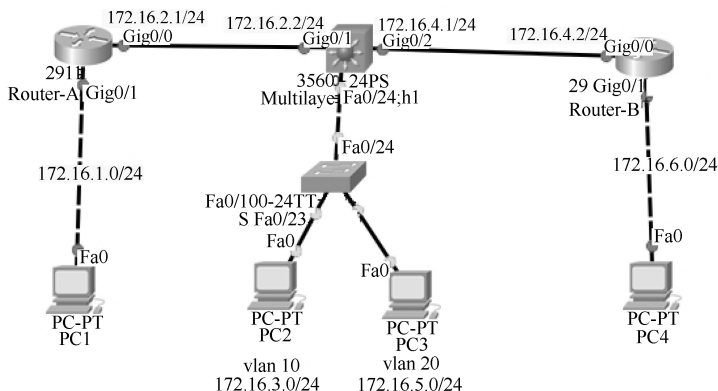


图 4-2-25 某公司拓扑图

完成标准：各网段能相互通信。

(2) 任务：配置 OSPF 单区域。

海天公司有两个分公司，公司网管采用了 OSPF 动态路由协议，如图 4-2-26 所示。

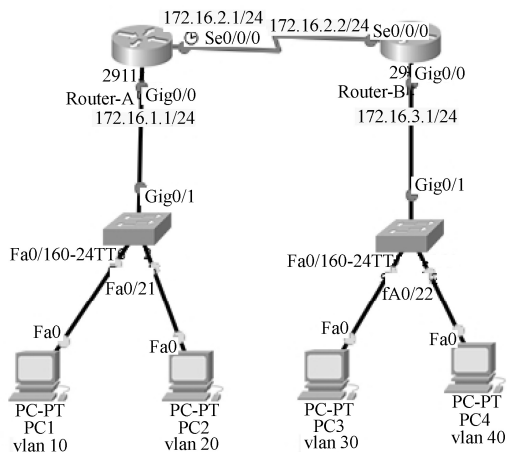


图 4-2-26 海天公司拓扑图



完成标准：各网段能相互通信。

(3) 任务：配置 OSPF 多区域。

某公司总部设在美国，中国分公司的网络通过路由器 Router-A 接入总部网络，加拿大分公司通过路由器 Router-B 接入总部网络。由于公司网络规模较大且设备的厂商不同，为了解决路由收敛速度和设备厂商的兼容性问题，该公司的网络管理员打算采用链路状态路由协议实现路由选择，如图 4-2-27 所示。

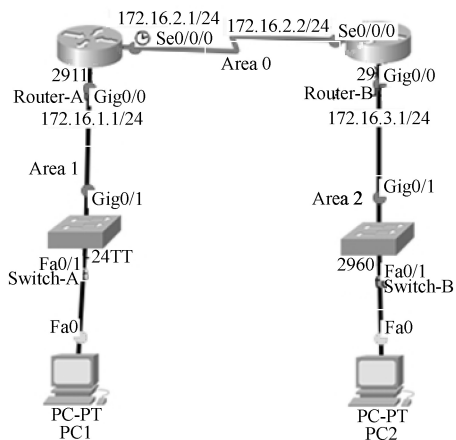
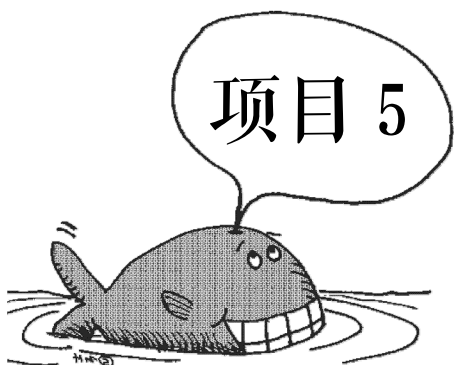


图 4-2-27 某公司拓扑图

完成标准：各网段能相互通信。



网络安全技术实现

项目学习说明

随着网络技术和应用范围的不断扩大，网络已经成为人们日常生活中必不可少的一部分。园区网作为给终端用户提供网络接入和基础服务的应用环境，其存在的网络安全隐患不断显现出来，如非人为的或自然力造成的故障、事故；人为但属于操作人员无意的失误造成的数据丢失或损坏；来自园区网外部和内部人员的恶意攻击和破坏。网络安全状况直接影响人们的学习、工作和生活，网络安全问题已经成为信息社会关注的焦点之一，因此需要实施网络安全防范。

保护园区网络安全的措施包括诸如在终端主机上安装防病毒软件，保护终端设备安全；利用交换机的端口安全功能，防止局域网内部的 MAC 地址攻击、ARP 攻击、IP/MAC 地址欺骗等攻击；利用 IP 访问控制列表对网络流量进行过滤和管理，从而保护子网之间的通信安全及敏感设备，防止非授权的访问；利用 NAT 技术从一定程度上为内网主机提供“隐私”保护；在网络出口部署防火墙，防范外网未经授权访问和非法攻击；建立保护内部网络安全的规章制度，保护内网设备的安全。

本项目重点学习交换机端口安全功能配置、IP 访问控制列表的配置与应用，以及 NAT 的配置与应用。

学习能力目标

实训 1：交换机端口安全配置。

实训 2：IP 访问控制列表。

实训 3：网络地址转换。



职业能力目标

- 熟悉交换机端口安全的功能与使用。
- 熟悉交换机端口安全功能的配置方法。
- 理解访问控制列表的工作原理和分类。
- 熟练掌握标准访问控制列表的配置方法。
- 熟练掌握扩展访问控制列表的配置方法。
- 熟练掌握命名方式访问控制列表的配置方法。
- 熟练掌握动态 NAPT 实现局域网访问 Internet 的配置方法。
- 熟练掌握使用 NAT 实现外网主机访问内网服务器的配置方法。

实训 1 交换机端口安全配置

通过 MAC 地址表记录连接到交换机端口的以太网 MAC 地址，并只允许某个 MAC 地址通过本端口通信。其他 MAC 地址发送的数据包通过此端口时，端口安全特性会阻止它。

学习情境

海成公司最近网络速度变慢，公司的网络管理员发现有些部门的员工私自带笔记本式计算机接入公司网络来下载电影，给公司正常的上网带来了负担，同时也给公司的网络安全带来了隐患。

情境分析

非授权的计算机接入网络会造成公司信息管理成本增加，不仅影响公司正常用户的网络使用，还会造成严重的网络安全问题。在接入交换机上配置端口安全功能，利用 MAC 地址绑定不仅可以解决非授权计算机影响正常网络使用的问题，还可以避免恶意的用户利用未绑定 MAC 地址的端口来实施的 MAC 地址泛洪攻击。

所需设备：

- (1) Cisco Catalyst 3560 三层交换机 1 台。
- (2) Cisco Catalyst 2960 二层交换机 1 台。
- (3) PC 4 台。
- (4) 直通线 4 条。
- (5) 交叉线 1 条。
- (6) Console 线 1 条。

实训拓扑结构如图 5-1-1 所示。

网络设备、PC 的 IP 地址及端口信息如表 5-1-1 所示。

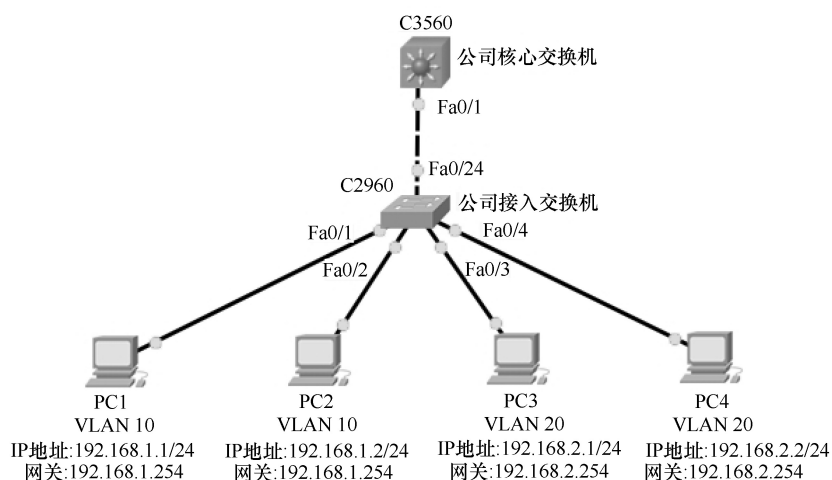


图 5-1-1 交换机端口安全配置

表 5-1-1 网络设备、PC 的 IP 地址及端口信息

设 备	端 口 成 员	IP 地址	子 网 掩 码	备 注
C3560 的 VLAN 0		192.168.1.254	255.255.255.0	
C3560 的 VLAN 20		192.168.2.254	255.255.255.0	
C3560	Fa0/1		255.255.255.0	Trunk
C2960 的 VLAN 10	Fa0/1		255.255.255.0	
	Fa0/2		255.255.255.0	
C2960 的 VLAN 20	Fa0/3		255.255.255.0	
	Fa0/4		255.255.255.0	
C2960	Fa0/24		255.255.255.0	Trunk
PC 1		192.168.1.1	255.255.255.0	MAC 地址: 000B.BE24.625A
PC 2		192.168.1.2	255.255.255.0	MAC 地址: 0009.7C90.B8B8
PC 3		192.168.2.1	255.255.255.0	MAC 地址: 00D0.9777.EA8C
PC 4		192.168.2.2	255.255.255.0	MAC 地址: 0001.43AA.3B92

步骤实现

步骤 1: 按照图 5-1-1 连接网络拓扑结构。

步骤 2: 按照表 5-1-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3: 配置交换机 C2960 的主机名称，创建 VLAN 10 和 VLAN 20，将 Fa0/1、2 划入 VLAN 10，Fa0/3、4 划入 VLAN 20，将 Fa0/24 配置为 Trunk。

```
Switch>enable
Switch#conf t
Switch(config)#hostname C2960
C2960(config)#vlan 10
C2960(config-vlan)#exit
C2960(config)#vlan 20
C2960(config-vlan)#exit
```



```
C2960(config)#int range f0/1-2
C2960(config-if-range)#switchport mode access
! 将端口设置为访问模式后，此端口才能启用 port-security 功能
C2960(config-if-range)#switchport access vlan 10
C2960(config-if-range)#exit
C2960(config)#int range f0/3-4
C2960(config-if-range)#switchport mode access
C2960(config-if-range)#switchport access vlan 20
C2960(config-if-range)#exit
C2960(config)#int f0/24
C2960(config-if)#switchport mode trunk
C2960(config-if)#exit
C2960(config)#
```



小贴士

基于中继链路协商的原则，C2960 通过配置 Trunk 来向 C3560 发送 DTP（动态中继协议）并与 C3560 协商中继链路，即只需在 C2960 设备（或 C3560）一端配置 Trunk 即可使中继链路协商成功。

步骤 4：配置交换机 C3560 的主机名称，创建 VLAN 10 和 VLAN 20，并 VLAN 10 和 VLAN 20 的 SVI 接口配置 IP 地址，并启用交换机的路由功能。

```
Switch>enable
Switch#conf t
Switch(config)#hostname C3560
C3560(config)#vlan 10
C3560(config-vlan)#exit
C3560(config)#vlan 20
C3560(config-vlan)#exit
C3560(config)#int vlan 10
C3560(config-if)#ip address 192.168.1.254 255.255.255.0
C3560(config-if)#no shutdown
C3560(config-if)#exit
C3560(config)#int vlan 20
C3560(config-if)#ip address 192.168.2.254 255.255.255.0
C3560(config-if)#no shutdown
C3560(config-if)#exit
C3560(config)#ip routing    ! 三层交换机必须启用路由功能才能实现 VLAN 间的通信
C3560(config)#
```

步骤 5：在交换机 C2960 上针对不同 VLAN 的主机配置端口安全。

```
C2960(config)#int range f0/1-2    ! 进入 VLAN 10 所在端口
C2960(config-if-range)#switchport port-security
! 将 f0/1 和 f0/2 端口启用端口安全功能
C2960(config-if-range)#switchport port-security maximum 1
! 设置端口的最大连接数为 1
C2960(config-if-range)#switchport port-security violation shutdown
```

! 设置违例处理方式为关闭端口

```
C2960(config-if-range)#switchport port-security mac-address sticky
```

! 设置基于黏性的安全 MAC 地址

```
C2960(config-if-range)#exit
```

```
C2960(config)#int f0/3      ! 进入 f0/3 端口
```

```
C2960(config-if)#switchport port-security      ! 将 f0/3 端口启用端口安全功能
```

```
C2960(config-if)#switchport port-security mac-address 00d0.9777.ea8c
```

! 将 f0/3 端口进行 MAC 地址绑定

```
C2960(config-if)#switchport port-security violation shutdown
```

! 设置违例处理方式为关闭端口

```
C2960(config-if)#exit
```

```
C2960(config)#int f0/4      ! 进入 f0/4 端口
```

```
C2960(config-if)#switchport port-security      ! 将 f0/4 端口启用端口安全功能
```

```
C2960(config-if)#switchport port-security mac-address 0001.43aa.3b92
```

! 将 f0/4 端口进行 MAC 地址绑定

```
C2960(config-if)#switchport port-security violation shutdown
```

! 设置违例处理方式为关闭端口

```
C2960(config-if)#exit
```

```
C2960(config)#
```



小贴士

在园区网内建议连接固定服务器的接口白名单使用手工配置, 连接常规 PC 的接口白名单采用自动学习, 但自动学习不能避免黑客盗用网线通过合法连接来进入内网进行攻击, 因此针对这种情况, 需要对连接常规 PC 的接口配置基于黏性的端口安全功能。

基于黏性的端口安全工作机制是当接口通过自动学习添加白名单时, 该白名单会以配置的形式保存在交换机上, 即便接口关闭后, 该接口原有的 MAC 地址表项删除了, 该白名单信息依然存在, 这样比较安全。

步骤 6: 测试园区网络通信及查看端口安全配置。

(1) 在 PC 1 上 ping PC 3 的 IP 地址, 可以连通, 说明可以正常工作, 如图 5-1-2 所示。

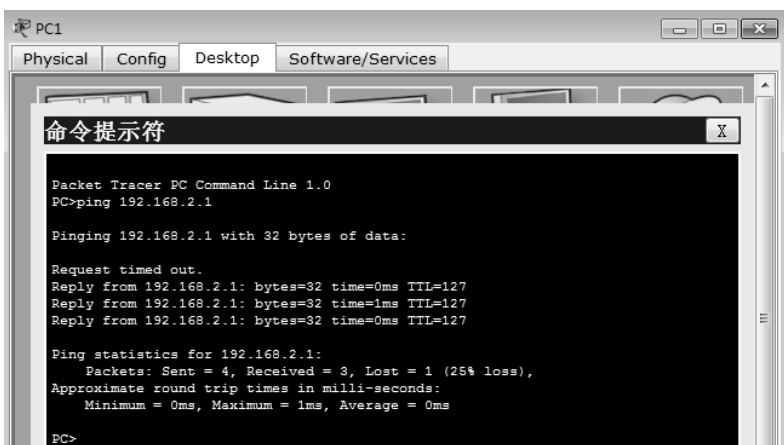


图 5-1-2 连通性测试效果图

(2) 查看交换机 C2960 的 MAC 地址表。执行端口安全功能的端口类型均为 Static (静



态）模式。

```
C2960#show mac-address-table
Mac Address Table
-----

Vlan Mac Address Type Ports
----
-----

1 0050.0f7a.c901 DYNAMIC Fa0/24
10 0009.7c90.b8b8 STATIC Fa0/2
10 000b.be24.625a STATIC Fa0/1
10 0090.2b79.a118 DYNAMIC Fa0/24
20 0001.43aa.3b92 STATIC Fa0/4
20 0090.2b79.a118 DYNAMIC Fa0/24
20 00d0.9777.ea8c STATIC Fa0/3
C2960#
```

(3) 查看交换机 C2960 的端口安全配置。

```
C2960#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)
-----

Fa0/1 1 1 0 Shutdown ! 端口安全已经配置
Fa0/2 1 1 0 Shutdown ! 端口安全已经配置
Fa0/3 1 1 0 Shutdown ! 端口安全已经配置
Fa0/4 1 1 0 Shutdown ! 端口安全已经配置
-----

C2960#
```

(4) 查看 fa0/1 的端口配置是否生效。

```
C2960#show port-security interface fa0/1
Port Security : Enabled ! 已开启
Port Status : Secure-up ! 已生效
Violation Mode : Shutdown ! 违例则关闭

Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 000B.BE24.625A:10
Security Violation Count : 0

C2960#
```

步骤 7: 端口安全功能测试, 发现 PC 1 和 PC 3 所连接的交换机端口都为 Shutdown。

(1) 单击 PC 1，打开 PC 1 窗口，选择“Config”→“接口配置”选项，在右侧的“FastEthernet0”中修改 PC 1 的 MAC 地址为“000B.BE24.6250”，如图 5-1-3 所示。

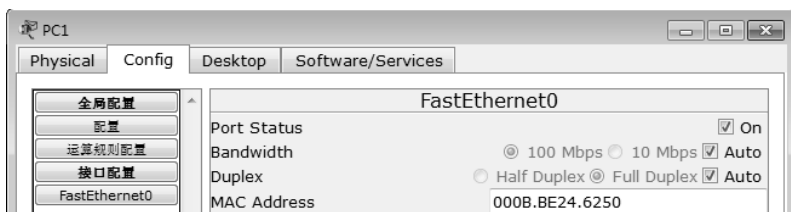


图 5-1-3 修改 PC1 的 MAC 地址

(2) 单击 PC 3，打开 PC 3 窗口，选择“Config”→“接口配置”选项，在右侧的“FastEthernet0”中修改 PC 3 的 MAC 地址为“00D0.9777.EA80”，如图 5-1-4 所示。

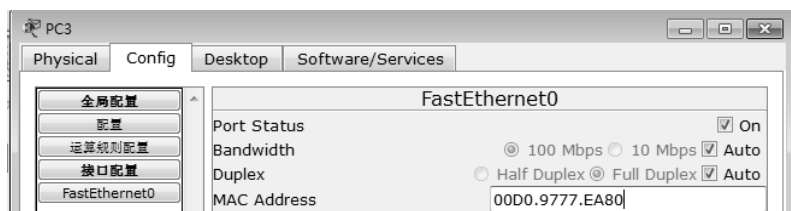


图 5-1-4 修改 PC3 的 MAC 地址

(3) 在 PC 1 上 ping PC 3 的 IP 地址，无法连通，说明无法正常工作，如图 5-1-5 所示。

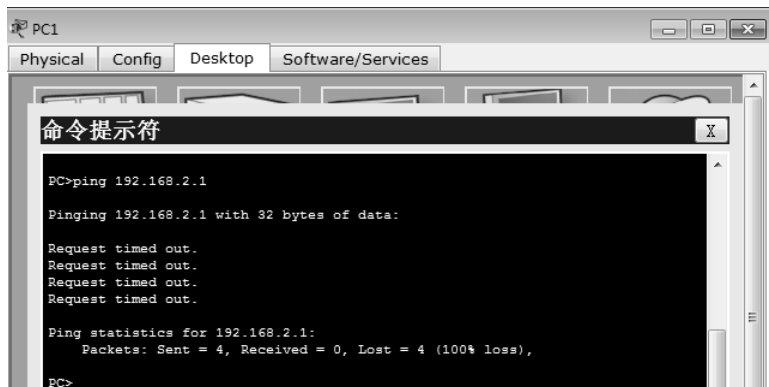


图 5-1-5 连通性测试效果图

(4) 查看 fa0/1 端口，发现已经为 Shutdown，说明端口安全已生效。

```
C2960#show port-security int fa0/1
Port Security : Enabled
Port Status : Secure-shutdown    ! 已变为 shutdown 状态
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
```



```
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 000B.BE24.6250:10
Security Violation Count : 1
```

C2960#



小贴士

当端口因违例而被关闭后，要恢复端口状态有如下两种方法。

(1) 在全局配置模式下使用“errdisable recovery”命令来将接口从错误状态恢复过来（模拟器不支持此功能）。

(2) 先将已关闭端口配置为 shutdown 之后再配置 no shutdown 即可。

相关知识

1. 端口安全

交换机的端口安全功能，是指针对交换机的端口进行安全属性的配置，从而控制用户的安全接入。端口安全特性可以使特定 MAC 地址的主机流量通过该端口。当端口上配置了安全的 MAC 地址后，定义之外的源 MAC 地址发送的数据包将被端口丢弃。交换机端口安全主要有两种类型：一是限制交换机端口的最大连接数；二是针对交换机端口进行 MAC 地址、IP 地址（可选）的绑定。

限制交换机端口的最大连接数可以控制交换机端口下连的主机数，并防止用户进行恶意 ARP 欺骗。

交换机端口的地址绑定，可以针对 MAC 地址、IP 地址（可选）、IP+MAC 地址（可选）进行灵活的绑定；可以对用户进行严格的控制，保证用户的安全接入和防止常见的内网的网络攻击。

安全的 MAC 地址类型有如下 3 种。

(1) 静态安全的 MAC 地址：手工配置，存储在 MAC 地址表内并加入到交换机的配置文件中。

(2) 动态安全的 MAC 地址：动态学习，只存储在 MAC 地址表中，交换机重启之后丢失。

(3) 粘性安全的 MAC 地址：可以动态学习，也可以手工配置，存储在 MAC 地址表内并加入到交换机的配置文件中，如果配置被保存，则即使交换机重启也无需重新配置。

安全 MAC 地址的老化时间：在没有为一个接口上的所有安全地址配置老化时间时，所有的安全地址永远不失效。但由于有些安全地址很长时间未访问端口，此安全地址由于没有失效还要占用安全端口的个数。如果设置了老化时间，在老化时间内，安全地址没有访问端口，则从安全地址表中将此安全地址删除，空出一个安全地址位置，以使其他地址成为安全地址。当设置安全地址的最大个数后，可以使交换机自动地增加和删除接口上的安全地址。安全 MAC 地址默认的老化时间为 300s。

若一个端口配置了 port-security，在其安全地址的数目已经达到允许的最大个数后，如果该端口再收到一个源地址不属于端口的安全地址的数据包时，安全违例将产生。

当安全违例产生时，处理方式有如下 3 种。

(1) protect：当安全地址个数满后，安全端口将丢弃未知名地址（不是该端口的安全地址中的任何一个）的包。

(2) restrict：当违例产生时，将发送一个 trap 通知。

(3) shutdown：当违例产生时，将关闭端口并发送一个 trap 通知。

当端口因违例而被关闭后，在全局配置模式下使用“errdisable recovery”命令来将接口从

错误状态恢复过来。

交换机端口安全的注意事项如下。

(1) 交换机端口安全功能只能配置在访问接口、干道接口和 IEEE 802.1Q 的隧道接口上,不能配置在动态接口上。

(2) 端口安全的接口不能是 SPAN 的目的接口。

(3) 端口安全的接口不能属于聚合链路端口组。

(4) 交换机最大连接数限制取值为 1~128,默认是 128。

(5) 交换机最大连接数限制默认的处理方式是 protect。

(6) 交换机不支持针对粘性安全 MAC 地址的老化。

2. 端口安全配置解析

(1) 开启端口安全。

```
Switch(config)#interface f0/1
Switch(config-if)# switchport port-security
```

(2) 配置端口安全地址的最大个数。

```
Switch(config-if)# switchport port-security maximum value
```

value 为安全地址的最大值,可为 1~128。

(3) 配置处理违例的方式。

```
Switch(config-if)# switchport port-security violation {protect | restrict | shutdown}
```

(4) 配置端口与 MAC 地址的绑定。

```
Switch(config-if)# switchport port-security [mac-address mac-address]
```

(5) 在 MAC 地址表中添加端口与 MAC 地址的绑定。

```
Switch(config)#mac-address-table static [mac-address] [vlan vlan-id] [interface interface-id]
```

(6) 开启粘性地址学习功能。

```
Switch(config-if)# switchport port-security mac-address sticky
```

(7) 配置安全地址的老化时间 (Cisco Packet Tracer 软件暂不支持此功能)。

```
Switch(config-if)# switchport port-security aging {static | time time}
```

static 表示老化时间将同时应用于手工配置的安全地址和自动学习的地址,否则只应用于自动学习的地址。

time 表示这个端口上安全地址的老化时间,单位是 s,默认为 300s。当用户设置此值为 0 时,地址老化功能将被关闭,学习到的地址将不会被老化。

(8) 查看端口安全信息。

```
Switch#show port-security interface [interface-id]    ! 查看接口的端口安全配置信息
Switch#show port-security address                    ! 查看安全地址信息
Switch#show port-security [interface-id] address      ! 显示某个接口上的安全地址信息
Switch#show port-security                            ! 显示所有安全端口的统计信息,包括最安全地址数、当前安全地址数及违例处理方式等
```

课堂训练

(1) 在交换机上的端口 fa 0/1 上应用端口安全功能,设置最大地址个数为 2,设置违例方式为 shutdown。

(2) 为交换机上的端口 fa 0/10 上应用端口安全功能,并配置一个安全地址:



1D01.1F0C.017A。

知识拓展

1. 交换机风暴控制

1) 概述

端口接收到过量的广播、未知名多播或未知名单播包时，数据包的广播风暴就会产生，导致报文传输延时增大和网络变慢。

可以分别针对广播、未知名多播或未知名单播数据流进行风暴控制。当接口接收到的广播、未知名多播或未知名单播包的速率超过设定的阈值时，设备将只允许通过所设定阈值带宽的报文，超出阈值部分的报文将被丢弃，直到数据流恢复正常，从而避免过量的泛洪报文进入局域网形成风暴。

2) 配置风暴控制

默认情况下，针对广播、多播和未知名单播的风暴控制功能均被关闭。

在接口配置模式下配置风暴控制，命令如下。

```
switch(config-if)#storm-control {broadcast|multicast|unicast} [{level percent | pps packets | rate-bps}]
```

broadcast: 打开对广播风暴的控制功能。

multicast: 打开对未知名多播风暴的控制功能。

unicast: 打开对未知名单播风暴的控制功能。

percent: 以带宽的百分比进行设置，如 20 表示带宽的 20% 。

packets: 以 pps 为单位进行设置，即 packets per second

Rate-bps: 允许的通过速率。

3) 查看风暴控制状态

查看风暴控制状态的命令如下。

```
switch#show storm-control [interface interface-id]
```

2. 交换机保护端口

1) 概述

在某些应用环境下，要求交换机上的部分端口间不能互相通信，这时可以通过将某些端口设置为保护口来达到目的。当将端口设为保护口之后，保护口之间无法通信，保护口与非保护口之间可以正常通信。

保护口有两种模式：一种是阻断保护口之间的二层交换，但允许保护口之间进行路由；另一种是同时阻断保护口之间的二层交换和阻断路由，在两种模式都支持的情况下，第一种模式将作为默认配置模式。

当两个保护口设为一个 SPAN 端口对时，SPAN 的源端口发送或接收的帧依然能够镜像到 SPAN 目的端口。

2) 配置保护端口

配置保护端口的命令如下。

```
switch(config-if)# switchport protected
```

3) 查看保护端口

查看保护端口的命令如下。

```
switch# show interfaces switchport
```

学习小结

本实训主要学习了交换机端口安全功能的启用，并且学习了如何配置端口安全功能中的

最大连接数与违例处理方式，以及端口与 MAC 地址的绑定，从而实现控制用户的安全接入，防止非法用户进行的网络攻击。

实训 2 IP 访问控制列表

IP 访问控制列表（Access Control List, ACL）用于对流经路由器或交换机的数据包根据一定的规则进行过滤，从而提高网络可管理性和安全性。其主要分为标准 IP 访问控制列表、扩展 IP 访问控制列表和命名访问控制列表等。本实训分为以下 3 个任务进行学习。

任务 1 标准访问控制列表的配置。

任务 2 扩展访问控制列表的配置。

任务 3 命名访问控制列表的配置。

任务 1 标准访问控制列表的配置

学习情境

海成公司分为经理部、财务部和销售部，分属 3 个不同的网段，3 个部门之间用路由器进行信息传递。为了安全起见，公司领导要求管理员对网络的数据流量进行控制，使销售部不能对财务部进行访问，但经理部可以对财务部进行访问。

情境分析

公司的财务部门涉及企业许多重要的财务信息和数据，因此保障公司管理部门的安全访问，减少普通部门对财务部的访问很有必要，这样可以尽可能地减少网络安全隐患。

在路由器上应用标准访问控制列表，对访问财务部的数据流量进行限制，禁止销售部访问财务部的数据流量通过，但对经理部的访问不做限制，从而达到保护财务部主机安全的目的。

所需设备：

(1) Cisco 2911 路由器 2 台。

(2) PC 3 台。

(3) 直通线 3 条。

(4) 交叉线 1 条。

(5) Console 线 1 条。

任务拓扑结构如图 5-2-1 所示。

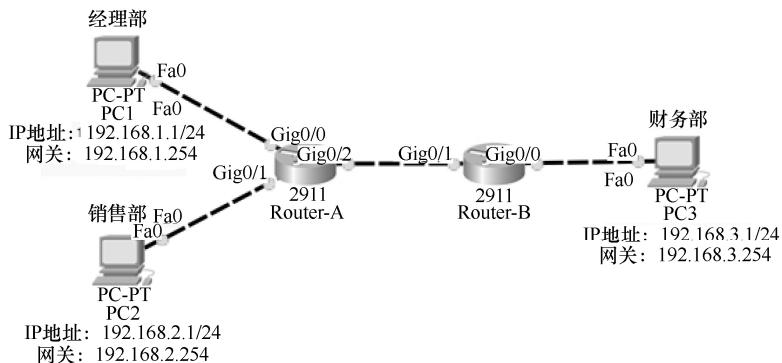


图 5-2-1 标准访问控制列表配置



路由器、PC 的 IP 地址及端口信息如表 5-2-1 所示。

表 5-2-1 路由器、PC 的 IP 地址及端口信息表

设 备	端 口	IP 地址	子 网 掩 码	默 认 网 关
Router-A	G0/0	192.168.1.254	255.255.255.0	
	G0/1	192.168.2.254	255.255.255.0	
	G0/2	192.168.10.1	255.255.255.0	
Router-B	G0/0	192.168.3.254	255.255.255.0	
	G0/1	192.168.10.2	255.255.255.0	
PC 1	Fa0	192.168.1.1	255.255.255.0	192.168.1.254
PC 2	Fa0	192.168.2.1	255.255.255.0	192.168.2.254
PC 3	Fa0	192.168.3.1	255.255.255.0	192.168.3.254

步骤实现

步骤 1：按照图 5-2-1 连接网络拓扑结构。

步骤 2：按照表 5-2-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：配置 Router-A 的主机名称和接口 IP 地址。

```
Router>enable
Router#config t
Router(config)#hostname Router-A
Router-A(config)#int g0/0
Router-A(config-if)#ip address 192.168.1.254 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config)#int g0/1
Router-A(config-if)#ip address 192.168.2.254 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config)#int g0/2
Router-A(config-if)#ip address 192.168.10.1 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config-if)#exit
Router-A(config)#
```

步骤 4：配置 Router-B 的主机名称和接口 IP 地址。

```
Router>enable
Router#config t
Router(config)#hostname Router-B
Router-B(config)#int g0/1
Router-B(config-if)#ip address 192.168.10.2 255.255.255.0
Router-B(config-if)#no shutdown
Router-B(config)#int g0/0
Router-B(config-if)#ip address 192.168.3.254 255.255.255.0
Router-B(config-if)#no shutdown
Router-B(config-if)#exit
Router-B(config)#
```

步骤 5：在 Router-A 和 Router-B 上配置静态路由。

```
Router-A(config)#ip route 192.168.3.0 255.255.255.0 192.168.10.2
Router-B(config)#ip route 192.168.1.0 255.255.255.0 192.168.10.1
Router-B(config)#ip route 192.168.2.0 255.255.255.0 192.168.10.1
```

步骤 6: 验证网络的连通性, 测试 PC 2 (销售部) 到 PC 3 (财务部) 的通信, 发现可以连通, 如图 5-2-2 所示。

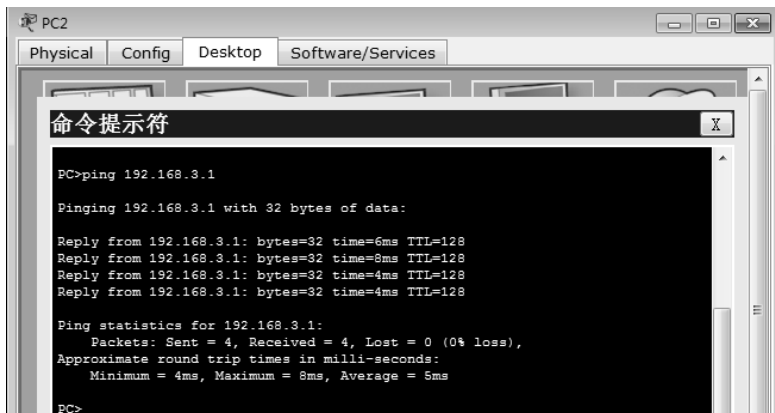


图 5-2-2 连通性测试效果图 (一)

步骤 7: 配置标准访问控制列表, 禁止 PC 2 (销售部) 访问 PC 3 (财务部)。

```

Router-B(config)#access-list 10 deny 192.168.2.0 0.0.0.255
! 配置标准 ACL 规则: 列表号为 10, 禁止 192.168.2.0 网段主机的流量通过
Router-B(config)#access-list 10 permit any      ! 允许其他流量
Router-B(config)#int g0/0      ! 进入端口
Router-B(config-if)#ip access-group 10 out
! 将访问控制列表应用到 Router-B 的 G0/0 端口的出口方向
Router-B(config-if)#exit
Router-B(config)#
  
```



小贴士

为了避免源主机所有流量 (包括正常通信流量) 均被禁止, 标准访问控制列表要应用在尽量靠近目的地址的接口上。

访问控制列表中的网络掩码是反掩码。

访问控制列表中默认有一条 “deny all” 语句, 因此列表中至少要有一条 “permit” 的条件语句。

步骤 8: 测试与查看访问控制列表信息。

(1) 测试 PC2 (销售部) 到 PC3 (财务部) 的连通性, 结果是无法连通的, 如图 5-2-3 所示。

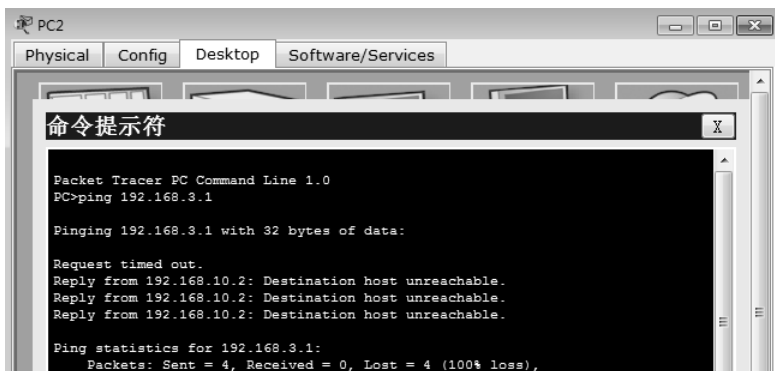


图 5-2-3 连通性测试效果图 (二)



(2) 查看访问控制列表信息。

```
Router-B#show access-lists 10
Standard IP access list 10
deny 192.168.2.0 0.0.0.255 (3 match(es))
permit any
Router-B#
```

相关知识

1. IP 访问控制列表

1) 概述

IP 访问控制列表用于对流经路由器或交换机的数据包根据一定的规则进行过滤，从而实现网络安全访问控制的目的。

2) 作用

- (1) ACL 可以限制网络流量、提高网络性能。
- (2) ACL 可以限制或减少路由更新的内容。
- (3) ACL 提供网络安全访问的基本手段。
- (4) ACL 检查和过滤数据包。

3) 工作原理

使用包过滤技术，在路由器或三层交换机上读取第 3 层或第 4 层包头中的信息，如源地址、目的地址、源端口、目的端口及上层协议等，根据预先定义的规则决定数据包的过滤，从而达到访问控制的目的，如图 5-2-4 所示。

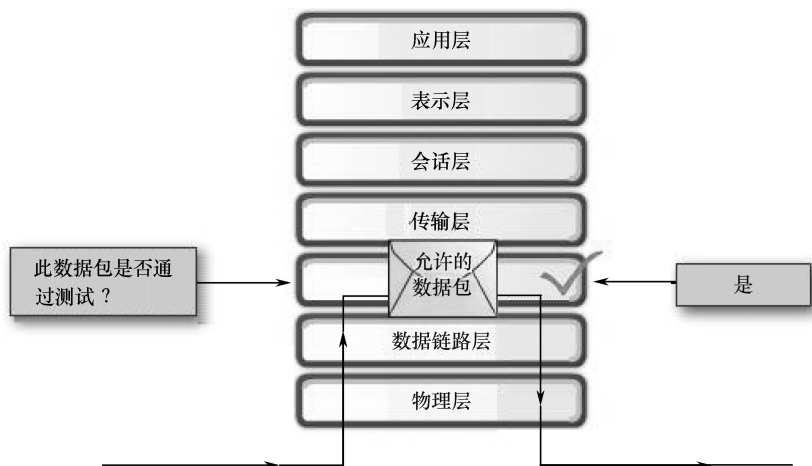


图 5-2-4 IP ACL 工作原理

例如，来自网络 A 的数据包使用端口 23 允许其通过，但会拒绝用户的其他访问，如图 5-2-5 所示。

定义访问控制列表的工作步骤，如图 5-2-6 所示。

- (1) 设置规则（哪些数据允许通过，哪些数据不允许通过）。
- (2) 执行规则。

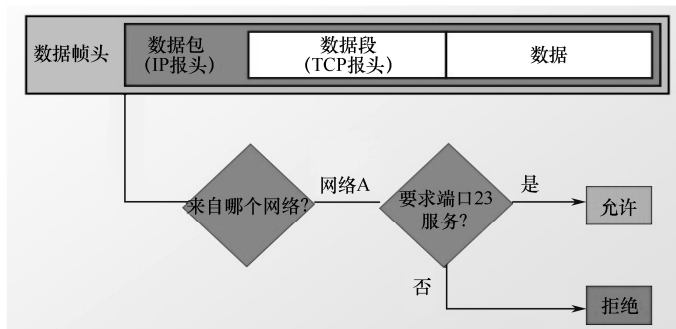


图 5-2-5 IP 流量访问控制

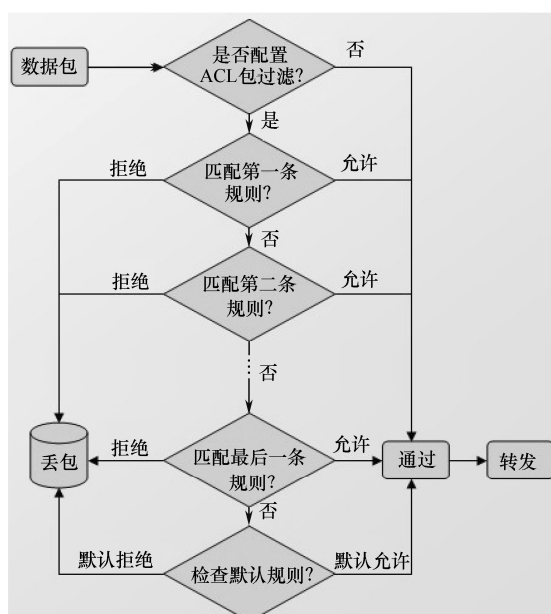


图 5-2-6 定义访问控制列表的工作步骤

4) IP 访问控制列表的分类

(1) 基本类型的访问控制列表有如下两类。

标准访问控制列表：只能通过 IP 数据包中的源 IP 地址进行过滤。

扩展访问控制列表：可以针对包括协议类型、源地址、目的地址、源端口、目的端口、TCP 连接建立等进行过滤。

(2) 其他类型的访问控制列表有如下两类。

命名访问控制列表：以列表名代替列表编号来定义 IP 访问控制列表，同样包括标准和扩展两种列表，定义过滤的语句与编号方式相似。

基于时间的访问控制列表：在原有的标准或扩展访问控制列表中，加入有效的时间范围来更合理地控制网络。

2. 标准访问控制列表

1) 概述

使用 1~99 及 1300~1999 中的数字作为访问控制列表编号，且只能通过 IP 数据包中的



源 IP 地址进行过滤。

2) 工作原理

当路由器收到一个数据包时，根据该数据包的源 IP 地址从访问控制列表的第一条语句开始逐条检查各语句。如果检查到匹配语句，则根据语句中是允许或禁止流量通过来处理该数据包；如果检查到最后还没有匹配的语句，则该数据包被丢弃。标准访问控制列表的工作过程如图 5-2-7 所示。

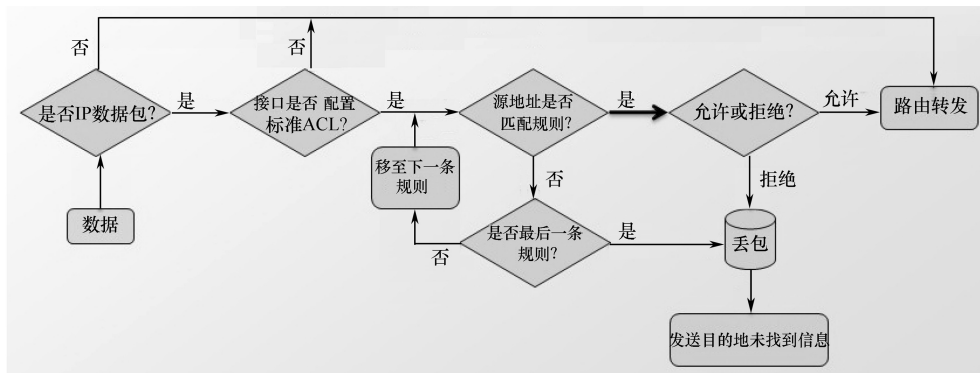


图 5-2-7 标准访问控制列表的工作过程

在标准或扩展访问控制列表的末尾，总有一个隐含的 **deny all** 语句。这意味着如果数据包源地址与任意允许语句不匹配，则隐含的 **deny all** 将会禁止该数据包通过。

3) 标准访问控制列表的配置

(1) 配置标准 ACL 规则。

```
Router(config)# access-list access-list-number { permit | deny } { any | source source-wildcard }
```

access-list-number: 表示访问控制列表的序号。

permit/deny: 表示访问控制是允许还是禁止满足条件的数据包通过。

Source: 表示被过滤数据包的源 IP 地址。

source-wildcard: 表示通配屏蔽码，1 表示不检查位，0 表示必须匹配位。

any/host: 表示任意主机或一台特定的主机。

(2) 应用标准 ACL 到接口。

```
Router(config-if)# ip access-group access-list-number { in | out }
```

in 表示应用到接口的入方向，对收到的报文进行检查。

out 表示应用到接口的外出方向，对发送的报文进行检查。

IP 访问控制列表只有被应用到某个接口才能达到报文过滤的目的。接口上通过的报文有两个方向，一个是通过接口进入路由器的报文，即 **in** 方向的报文；一个是通过接口离开路由器的报文，即 **out** 方向的报文，**out** 也是访问控制列表的默认方向。路由器一个接口的一个方向上只能应用一个 IP 访问控制列表。

(3) 删除已建立的标准 ACL。

```
Router(config)# no access-list access-list-number
```

(4) 显示访问控制列表配置。

```
Router# show access-list access-list-number
```

access-list-number 是可选参数，如果指定，则显示指定编号的访问控制列表配置细节；如果不指定，则显示所有访问控制列表的配置细节。

课堂训练

- (1) 定义标准 ACL 命令：定义访问控制列表 10，允许 192.168.2.0 网段的流量通过。
- (2) 定义标准 ACL 命令：定义访问控制列表 20，只禁止 192.168.3.0 网段的流量通过，并将该列表应用到路由器的 F0/1 端口的出栈方向上。
- (3) 定义标准 ACL 命令：定义访问控制列表 30，只禁止 IP 地址为 172.16.4.1 的计算机的流量通过，而 172.16.4.0 网段中的其他计算机可以正常访问，并将该访问控制列表应用到路由器的 F0/0 端口的入栈方向上。

学习小结

本任务介绍了通过配置标准访问控制列表，实现对公司安全级别较高的部门的网络安全访问控制。标准访问控制列表占用路由器资源很少，是一种最基本、最简单的访问控制列表格式，应用比较广泛，经常在要求控制级别较低的情况下使用。但标准访问控制列表只能通过 IP 数据包中的源 IP 地址进行过滤，而更加复杂的控制数据包的传输需要使用扩展访问控制列表来实现。

任务 2 扩展访问控制表的配置

学习情境

海成公司由于业务规模的扩大，架设了 FTP 和 Web 服务器，FTP 服务只供行政部门访问使用，Web 服务器则行政部门和职工宿舍都能访问，其余针对服务器的访问均被拒绝。公司局域网络通过三层交换机进行信息传递，通过配置实现网络数据流量的控制。

情境分析

从公司需求上看，标准访问控制列表是无法实现所需功能的，只能使用扩展 IP 访问控制列表。在三层交换机上应用扩展访问控制列表，对访问服务器的数据流量进行控制。禁止职工宿舍访问 FTP 服务器的数据流通过，但同时服务器又向公司所有用户提供了 Web 服务，而除此之外对服务器的其他访问均被拒绝，从而达到保护服务器和数据安全的目的。

所需设备：

- (1) Cisco 3560-24PS 三层交换机 1 台。
- (2) PC 2 台，服务器 1 台。
- (3) 直通线 3 条。
- (4) Console 线 1 条。

任务拓扑结构如图 5-2-8 所示。

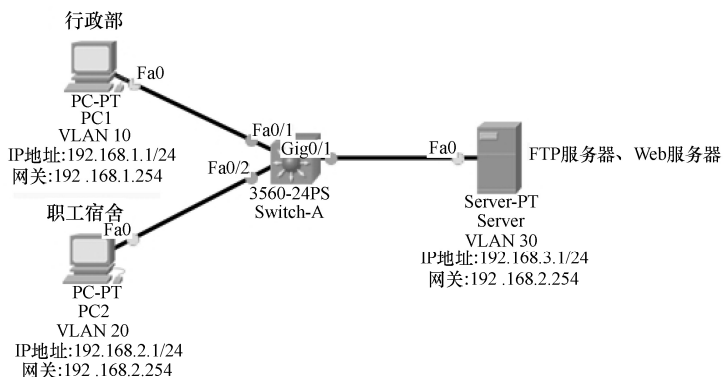


图 5-2-8 扩展访问控制列表配置



交换机、PC 的 IP 地址及端口信息如表 5-2-2 所示。

表 5-2-2 交换机、PC 的 IP 地址及端口信息表

设 备	接 口	IP 地址	子 网 掩 码	默 认 网 关
Switch-A 的 VLAN 10	Fa0/1	192.168.1.254	255.255.255.0	
Switch-A 的 VLAN 20	Fa0/2	192.168.2.254	255.255.255.0	
Switch-A 的 VLAN 30	G0/1	192.168.3.254	255.255.255.0	
PC 1	VLAN 10	192.168.1.1	255.255.255.0	192.168.1.254
PC 2	VLAN 20	192.168.2.1	255.255.255.0	192.168.2.254
Server	VLAN 30	192.168.3.1	255.255.255.0	192.168.3.254

步骤实现

步骤 1：按照图 5-2-8 连接网络拓扑结构。

步骤 2：按照表 5-2-2 配置计算机和服务器的 IP 地址、子网掩码和网关。

步骤 3：配置 Switch-A 的主机名称，创建 VLAN 10、20 和 30，并将 Fa0/1 划入 VLAN 10，Fa0/2 划入 VLAN 20，G0/1 划入 VLAN 30。

```
Switch(config)#hostname Switch-A
Switch-A(config)#vlan 10
Switch-A(config-vlan)#exit
Switch-A(config)#vlan 20
Switch-A(config-vlan)#exit
Switch-A(config)#vlan 30
Switch-A(config-vlan)#exit
Switch-A(config)#int fa0/1
Switch-A(config-if)#switchport mode access
Switch-A(config-if)#switchport access vlan 10
Switch-A(config)#int fa0/2
Switch-A(config-if)#switchport mode access
Switch-A(config-if)#switchport access vlan 20
Switch-A(config)#int g0/1
Switch-A(config-if)#switchport mode access
Switch-A(config-if)#switchport access vlan 30
Switch-A(config-if)#exit
Switch-A(config)#
```

步骤 4：在 Switch-A 上为 VLAN 10、VLAN 20 和 VLAN 30 的 SVI 接口配置 IP 地址，并启用交换机的路由功能。

```
Switch-A(config)#int vlan 10
Switch-A(config-if)#ip address 192.168.1.1 255.255.255.0
Switch-A(config-if)#no shutdown
Switch-A(config)#int vlan 20
Switch-A(config-if)#ip address 192.168.2.1 255.255.255.0
Switch-A(config-if)#no shutdown
Switch-A(config)#int vlan 30
Switch-A(config-if)#ip address 192.168.3.1 255.255.255.0
```

```
Switch-A(config-if)#no shutdown
Switch-A(config-if)#exit
Switch-A(config)#ip routing
```

步骤 5: 测试 PC 2 到服务器的应用访问。

(1) 测试 PC 2 (职工宿舍) 到 FTP 的访问, 发现是可以访问的, 如图 5-2-9 所示。

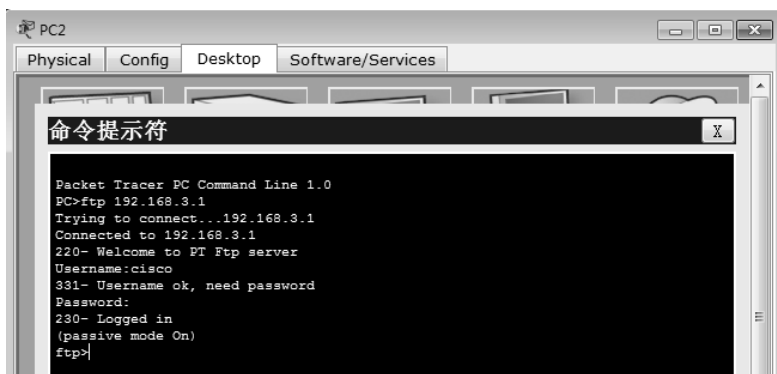


图 5-2-9 测试到 FTP 服务器的访问

(2) 测试 PC 2 (职工宿舍) 到 Web 的访问, 发现是可以访问的, 如图 5-2-10 所示。

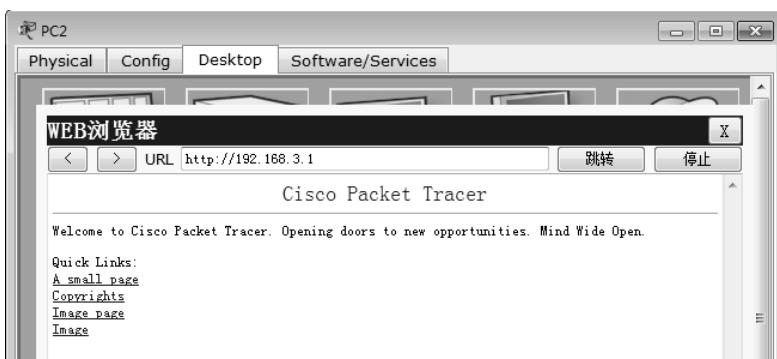


图 5-2-10 测试到 Web 服务器的访问



小贴士

模拟器中的 FTP 和 Web 服务器默认已经搭建好, 访问地址为服务器的 IP 地址。

模拟器中的 FTP 连接验证是在 PC 的命令提示符中输入 “>ftp 服务器 IP 地址”, 并输入默认的用户名和密码 (均为 cisco), 登录并查看。

步骤 6: 配置扩展访问控制列表, 针对服务器的访问流量进行控制。

```
Switch-A(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.255 host
192.168.3.1 eq 21          ! 定义扩展 ACL, 允许行政部对 FTP 的访问
Switch-A(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.255 host
192.168.3.1 eq 20          ! 定义扩展 ACL, 允许行政部对 FTP 的访问
Switch-A(config)#access-list 101 permit tcp 192.168.1.0 0.0.0.255 host
192.168.3.1 gt 1024        ! 定义扩展 ACL, 允许行政部对服务器端口号在 1024 以上的 TCP 流量通
! 过, 此规则主要针对在 PASV 模式下允许 FTP 数据传输
Switch-A(config)#access-list 101 permit tcp 192.168.0.0 0.0.255.255 host
```



```
192.168.3.1 eq www      ! 定义扩展 ACL，允许公司各部门对 Web 服务器进行访问
Switch-A(config)#access-list 101 deny ip any any      ! 禁止其他数据流量
Switch-A(config)#int vlan 30      ! 进入服务器所在 VLAN
Switch-A(config-if)#ip access-group 101 out      ! 将 ACL 应用到 VLAN 30 的出口方向
Switch-A(config-if)#exit
```



小贴士

FTP 一般是有两个连接的：一个用于客户机和服务器传输命令，即 21 端口；另一个用于数据传送的连接，即 20 端口。FTP 服务程序一般会支持两种不同的模式，一种是 Port 模式，另一种是 Passive 模式。当 FTP 连接在端口模式下出现“建立数据 socket 失败”时，可在 PASV 模式下使用高于 1024 的任一个空闲端口传输数据。

VLAN 的访问控制列表要在 VLAN 的 SVI 接口下应用。

为了减少被拒绝流量占用的带宽，扩展访问控制列表要应用在尽量靠近源地址的接口。

步骤 7：测试公司各部门到 PC3（服务器）的应用访问。

(1) 测试 PC 1（行政部）到 FTP 服务器的访问，发现是可以访问的，如图 5-2-11 所示。

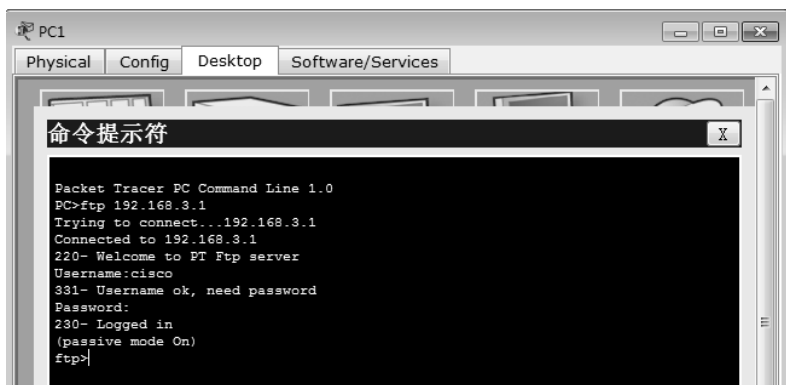


图 5-2-11 PC1 到 FTP 服务器的访问

(2) 测试 PC 1（行政部）到 PC 3（服务器）的连通性，发现是无法连通的，如图 5-2-12 所示。

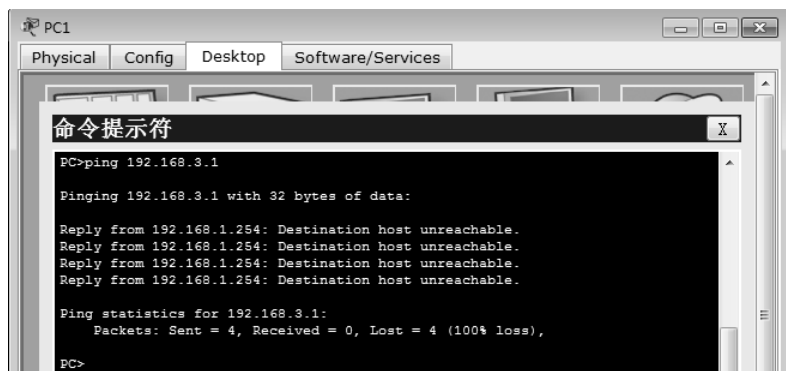


图 5-2-12 PC 1 到 PC 3 的访问

(3) 测试 PC 1（行政部）到 PC 3（服务器）的 Web 的访问，发现是可以连通的，如图 5-2-12 所示。

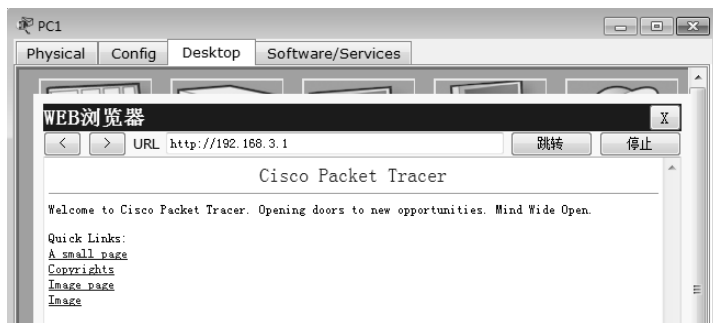


图 5-2-13 PC 1 到 PC 3 的访问

(4) 测试 PC 2（职工宿舍）对 FTP 的访问，发现是不能访问的，如图 5-2-14 所示。

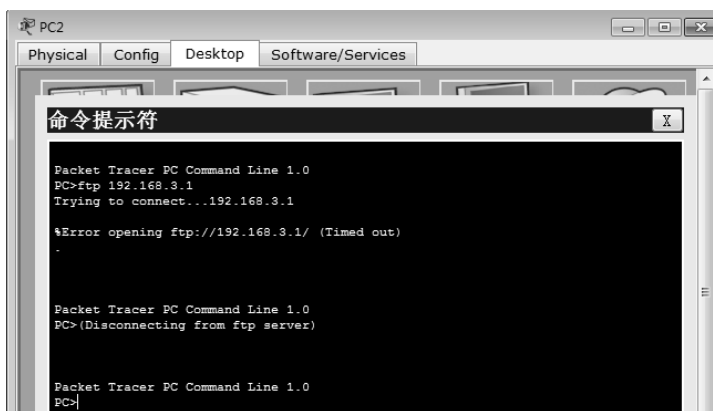


图 5-2-14 PC 2 对 FTP 服务器的访问

(5) 测试 PC 2（职工宿舍）对 Web 的访问，发现是可以访问的，如图 5-2-15 所示。

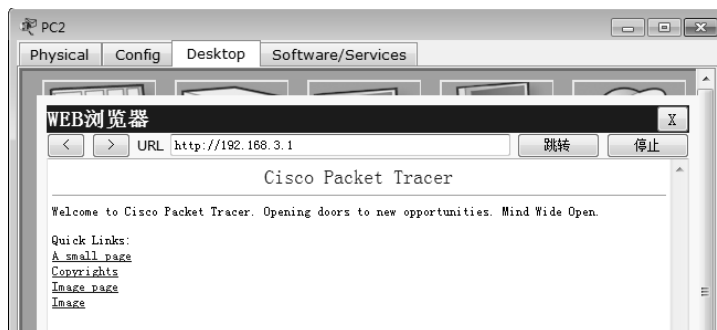


图 5-2-15 PC 2 对 Web 服务器的访问

步骤 8: 查看访问控制列表信息。

```

Switch-A#show access-lists 101
Extended IP access list 101
permit tcp 192.168.1.0 0.0.0.255 host 192.168.3.1 eq ftp (10 match(es))
permit tcp 192.168.1.0 0.0.0.255 host 192.168.3.1 eq 20
permit tcp 192.168.1.0 0.0.0.255 host 192.168.3.1 gt 1024
permit tcp 192.168.0.0 0.0.255.255 host 192.168.3.1 eq www (10 match(es))
  
```



```
deny ip any any (40 match(es))
```

```
Switch-A#
```

相关知识

1. 扩展访问控制列表

扩展访问控制列表使用 100~199 及 2000~2699 中的数字作为访问控制列表编号，可通过 IP 数据包中的源 IP 地址、目的 IP 地址、协议类型、源端口、目的端口等进行过滤，常用于高级的、精确的访问控制。

1) 工作原理

当路由器收到一个数据包时，路由器根据数据包的源 IP 地址、目的 IP 地址、协议类型、源端口、目的端口等从访问控制列表中自上而下检查控制语句。如果检查到其与一条 permit 语句匹配，则允许该数据包通过；如果检查到其与一条 deny 语句匹配，则该数据包被丢弃；如果检查到最后一条语句后还没有找到匹配的，则该数据包也将被丢弃。一旦控制列表允许数据包通过，路由器将数据包的目的网络地址与路由器上的内部路由器表相比较，将数据包路由到它的目的地。扩展访问控制列表的工作过程如图 5-2-16 所示。

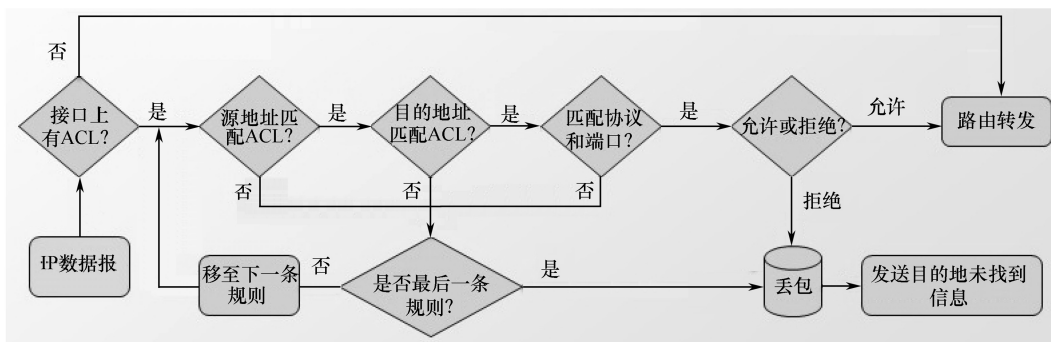


图 5-2-16 扩展访问控制列表的工作过程

2) 扩展访问控制列表的配置

(1) 配置扩展 ACL 规则：

```
Router(config)# access-list access-list-number { deny | permit } protocol  
{ any | source  
  source-wildcard } [ operator port ] { any | destination destination-  
wildcard } [ operator port ]
```

access-list-number：访问控制列表的编号，扩展访问控制列表的编号为 100~199 或 2000~2699

deny|permit：对符合匹配语句的数据包采取的动作，其中，permit 允许数据包通过，deny 拒绝数据包通过。

Protocol：数据包采用的协议，可以是 0~255 中的任意协议号，如 IP、TCP、UDP、IGMP 等。

source-address：数据包的源地址，可以是某个网络、某个子网或者某台主机。

source-wildcard：数据包源地址的通配符掩码。

destination-address：数据包的目的地址，可以是某个网络、某个子网或者某台主机

destination-wildcard：数据包目的地址的通配符掩码。

Operator：指定逻辑操作，可以是 eq（等于）、neq（不等于）、gt（大于）、lt（小于）或者是一个 range（范围）。

Port: 指定被匹配的应用层端口号，默认为全部端口号 0~65535，只有 TCP 和 UDP 需要指定端口范围，如 Telnet 为 23、Web 为 80、FTP 为 20 和 21 等。

常见的保留 TCP/UDP 端口号如表 5-2-3 所示。

表 5-2-3 常见的保留 TCP/UDP 端口号

端口号	关键字	描 述	端口号	关键字	描 述
7	ECHO	回显	25	smtp	简单邮件传输协议
20	ftp-data	文件传输协议（数据）	53	dns	域名服务
21	ftp	文件传输协议（控制）	69	tftp	简单文件传输协议
23	telnet	终端连接	80	http	超文本传输协议

(2) 在接口上应用标准 ACL:

```
Router(config-if)#ip access-group access-list-number { in | out }
```

注意：尽量将扩展 ACL 放置在靠近被拒绝的数据源的位置，这样可以减少被拒绝流量占用的带宽。

(3) 删除已建立的标准 ACL:

```
Router(config)# no access-list access-list-number
```

(4) 显示访问控制列表配置:

```
Router#show access-list access-list-number
```

课堂训练

(1) 定义扩展 ACL 命令：在路由器 Router 上定义访问控制列表 101，只允许 192.168.1.0 网段的主机向 201.1.1.0 网段的主机发送 WWW 报文，禁止其他报文通过，并将该列表应用到路由器的 F0/1 端口的出栈方向上。

(2) 定义扩展 ACL 命令：在三层交换机 Switch 上定义访问控制列表 110，禁止 172.16.3.0 网段（VLAN 30）的主机访问 172.16.4.0 网段（VLAN 40）的计算机，但可以访问 172.16.4.13 上的 WWW 服务，而其他服务不能访问，并将该列表应用到三层交换机的 VLAN 30 的 SVI 端口输入方向上。

学习小结

本任务介绍了如何配置扩展访问控制列表，实现针对不同部门或用户对公司服务器的网络安全访问控制。扩展访问控制列表功能很强大，但它存在一个缺点，即在没有硬件 ACL 加速的情况下，扩展 ACL 会消耗大量的路由器 CPU 资源。所以当使用中低档路由器时应尽量减少扩展 ACL 的条目数，即将其简化为标准 ACL 或将多条扩展 ACL 合为一条。

任务 3 命名访问控制列表的配置

学习情境

海成公司架设了两台服务器，分别为公司相关用户提供 FTP 服务和 Web 服务，FTP 服务器只为行政部提供服务，Web 服务器为公司用户提供网站访问服务，针对服务器的其他访问流都能通过。公司局域网络通过三层交换机进行信息传递，通过配置实现网络数据流量控制。

情境分析

为了提高网络管理效率，方便日后识别和管理不同部门的访问策略，可以考虑在部署网络安全访问策略时以命名控制列表来完成。

所需设备:

(1) Cisco 2911 路由器 2 台。



(2) Cisco Catalyst 2960 交换机 1 台。

(3) PC 2 台，服务器 2 台。

(4) 直通线 3 条。

(5) 交叉线 3 条。

(6) Console 线 1 条。

任务拓扑结构如图 5-2-17 所示。

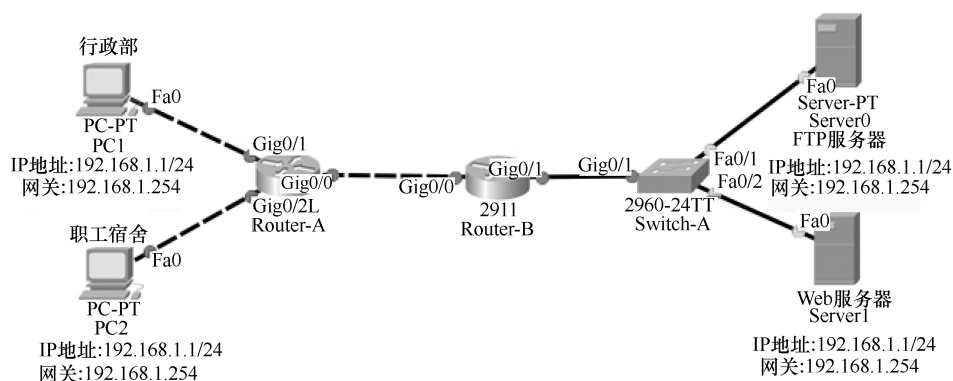


图 5-2-17 命名访问控制列表配置

网络设备、PC 的 IP 地址及端口信息如表 5-2-4 所示。

表 5-2-4 IP 地址及端口信息表

设 备	接 口	IP 地址	子 网 掩 码	默 认 网 关
Router-A	G0/0	192.168.10.1	255.255.255.0	
	G0/1	192.168.1.254	255.255.255.0	
	G0/2	192.168.2.254	255.255.255.0	
Router-B	G0/0	192.168.10.2	255.255.255.0	
	G0/1	192.168.3.254	255.255.255.0	
PC 1		192.168.1.1	255.255.255.0	192.168.1.254
PC 2		192.168.2.1	255.255.255.0	192.168.2.254
FTP 服务器		192.168.3.1	255.255.255.0	192.168.3.254
Web 服务器		192.168.3.2	255.255.255.0	192.168.3.254

步骤实现

步骤 1：按照图 5-2-17 连接网络拓扑结构。

步骤 2：按照表 5-2-4 配置计算机和服务器的 IP 地址、子网掩码和网关。

步骤 3：配置 Router-A 的主机名称及其接口 IP 地址。

```
Router>enable
ROUTER#conf t
Router-A(config)#hostname Router-A
Router-A(config)#int g0/1
Router-A(config-if)#ip address 192.168.1.254 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config)#int g0/2
Router-A(config-if)#ip address 192.168.2.254 255.255.255.0
```

```

Router-A(config-if)#no shutdown
Router-A(config)#int g0/0
Router-A(config-if)#ip address 192.168.10.1 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config-if)#exit
Router-A(config)#

```

步骤 4: 配置 Router-B 的主机名称及其接口 IP 地址。

```

Router>enable
ROUTER#conf t
Router(config)#hostname Router-B
Router-B(config)#int g0/0
Router-B(config-if)#ip address 192.168.10.2 255.255.255.0
Router-B(config-if)#no shutdown
Router-B(config-if)#exit
Router-B(config)#int g0/1
Router-B(config-if)#ip address 192.168.3.254 255.255.255.0
Router-B(config-if)#no shutdown
Router-B(config-if)#exit

```

步骤 5: 在路由器上配置静态路由, 实现各部门间的通信。

```

Router-A(config)#ip route 192.168.3.0 255.255.255.0 192.168.10.2
Router-B(config)#ip route 192.168.1.0 255.255.255.0 192.168.10.1
Router-B(config)#ip route 192.168.2.0 255.255.255.0 192.168.10.1

```

步骤 6: 测试 PC 2 (职工宿舍) 到服务器的通信。

(1) 测试 PC 2 (职工宿舍) 到 FTP 的访问, 发现是可以访问的, 如图 5-2-18 所示。

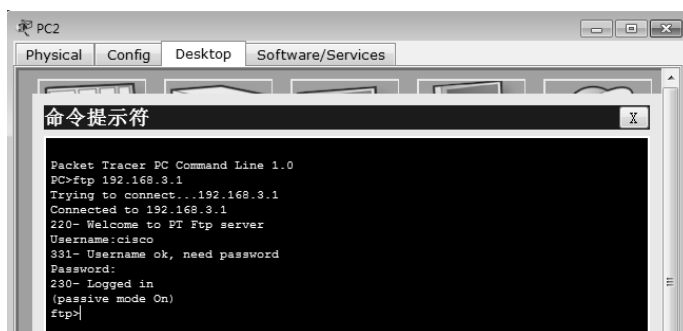


图 5-2-18 测试到 FTP 服务器的访问

(2) 测试 PC 2 (职工宿舍) 到 Web 的访问, 发现是可以访问的, 如图 5-2-19 所示。

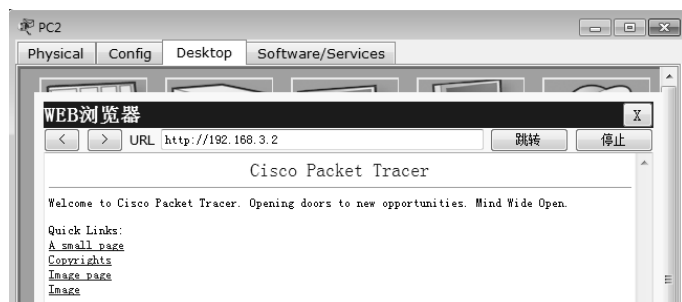


图 5-2-19 测试到 Web 服务器的访问



步骤 7：配置基于命名方式的扩展访问控制列表，针对网管中心服务器的访问流量进行控制。

```
Router-A(config)#ip access-list extended Web-ftp-service
! 定义基于命名方式的扩展 ACL

Router-A(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255 eq 21
! 定义扩展 ACL 规则：允许行政部主机对网管中心的 FTP 服务器进行访问控制流量

Router-A(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255 eq 20
! 定义扩展 ACL 规则：允许行政部主机对网管中心的 FTP 服务器进行传输流量

Router-A(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 192.168.3.0
0.0.0.255 gt 1024
! 定义扩展 ACL 规则：允许行政部主机对网管中心端口号大于 1024 的 TCP 流量

Router-A(config-ext-nacl)#permit tcp 192.168.0.0 0.0.255.255 192.168.3.0
0.0.0.255 eq 80
! 定义扩展 ACL 规则：允许公司各部门主机对网管中心的 Web 访问

Router-A(config-ext-nacl)#deny ip any any ! 拒绝其他对网管中心的访问流量

Router-A(config-ext-nacl)#exit
Router-A(config)#int g0/0 ! 进入端口

Router-A(config-if)#ip access-group Web-ftp-service out
! 在 Router-A 的 G0/0 端口的出口方向应用命名扩展 ACL

Router-A(config-if)#exit
```

步骤 8：测试公司各部门到服务器的应用访问。

(1) 测试 PC 2（职工宿舍）到 FTP 的访问，发现是不能访问的，如图 5-2-20 所示。

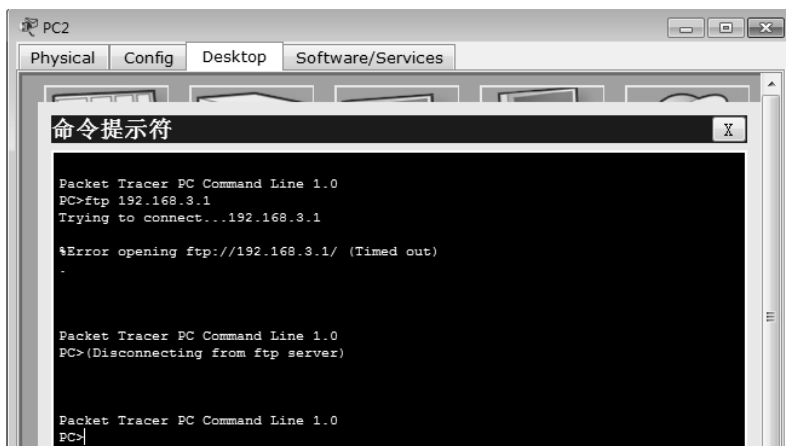


图 5-2-20 PC 2 对 FTP 服务器的访问

(2) 测试 PC 2（职工宿舍）到 Web 的访问，发现是可以访问的，如图 5-2-21 所示

(3) 测试 PC 1（行政部门）到 FTP 的访问，发现是可以访问的，如图 5-2-22 所示。

(4) 测试 PC 1（行政部门）到服务器的连通性，发现是无法连通的，如图 5-2-23 所示。

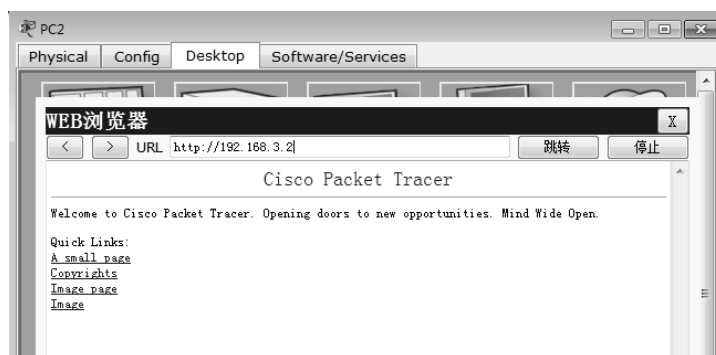


图 5-2-21 PC 2 对 Web 服务器的访问

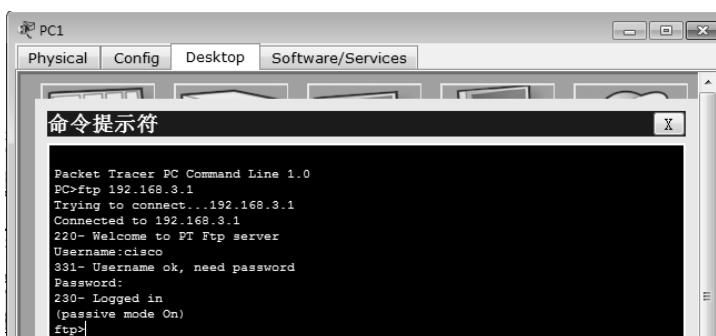


图 5-2-22 PC 1 对 FTP 服务器的访问

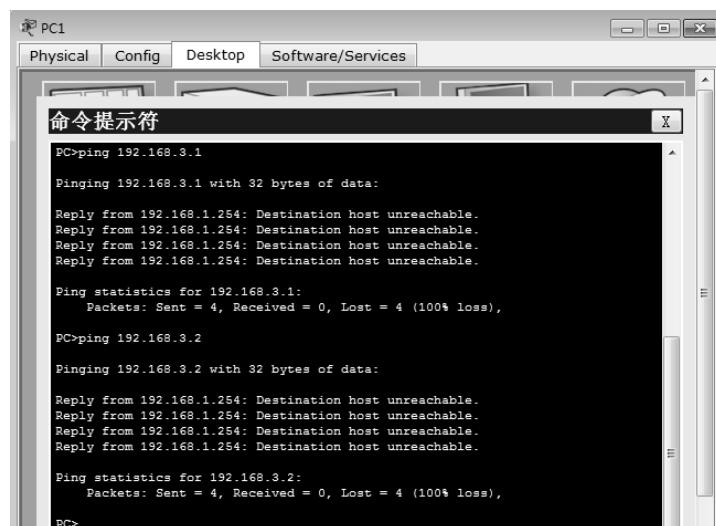


图 5-2-23 PC 1 到服务器的连通性

步骤 9: 查看访问控制列表信息。

```

Router-A#show access-lists web-ftp-service
Extended IP access list web-ftp-service
permit tcp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 eq ftp (11 match(es))
permit tcp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 eq 20
  
```



```
permit tcp 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255 gt 1024
permit tcp 192.168.0.0 0.0.255.255 192.168.3.0 0.0.0.255 eq www (7 match(es))
deny ip any any (8 match(es))
Router-A#
```

相关知识

1. 命名访问控制列表

在标准访问控制列表和扩展访问控制列表中使用一个字母数字组合的字符串（名称）代替前面使用的数字来表示访问控制列表的表号，便于识别编制的访问控制列表规则内容的功能。

（1）基于编号的访问控制列表和基于命名的访问控制列表的主要区别如下。

- ① 命名访问控制列表能更直观地反映出访问控制列表完成的功能。
- ② 命名访问控制列表能够定义更多的访问控制列表。
- ③ 单个路由器上命名访问控制列表的名称在所有协议和类型的命名访问控制列表中必须是唯一的，而不同路由器上的命名访问控制列表名称可以相同。
- ④ 命名访问控制列表是一个全局命令，它使用户进入到命名 **IP** 列表的子模式，在该子模式下建立匹配和允许/拒绝动作的相关语句。
- ⑤ 命名访问控制列表允许删除个别语句，当一个命名访问控制列表中的语句要被删除时，只需将该语句删除；而编号访问控制列表中则需要将访问控制列表中的所有语句都删除后再重新输入。

⑥ 命名访问控制列表的命令为 **ip access-list**，在命令中用 **standard** 和 **extended** 来区别标准访问控制列表和扩展访问控制列表；而编号访问控制列表的配置命令为 **access-list**，并用编号来区别标准和扩展访问控制列表。

（2）基于命名的标准访问控制列表的配置。

① 定义标准 **ACL** 名称：

```
Router(config)# ip access-list standard { name }
```

② 配置 **ACL** 规则：

```
Router(config-std-nacl)# { permit | deny } { any | source source-wildcard }
```

③ 应用 **ACL** 规则：

```
Router(config-if)# ip access-group { name } { in | out }
```

④ 显示访问控制列表配置

```
Router#show access-lists { aclname }
```

（3）基于命名的扩展访问控制列表的配置。

① 定义扩展 **ACL** 名称：

```
Router(config)# ip access-list extended { name }
```

② 配置 **ACL** 规则：

```
Router(config-ext-nacl)# { permit | deny } protocol { any | source source-wildcard } [ operator port ] { any | destination destination-wildcard } [ operator port ]
```

③ 应用 **ACL** 规则：

```
Router(config-if)# ip access-group { name } { in | out }
```

④ 显示访问控制列表的配置：

```
Router#show access-lists { aclname }
```

课堂训练

(1) 定义命名标准 ACL 命令：在路由器上配置命名标准 ACL，定义 ACL 名称为 test，拒绝 192.168.2.0 网段的所有流量通过，但允许其他流量通过，并将该列表应用到路由器的 F0/1 端口的出栈方向上。

(2) 定义命名扩展 ACL 命令：在三层交换机上配置命名扩展 ACL，只允许 192.168.2.0 网段上的主机访问 IP 地址为 192.168.1.254 的 Web 服务器，而禁止其他任意主机访问该服务器，并将该列表应用到三层交换机的 VLAN 20 的入口方向上。

学习小结

本任务主要学习如何配置基于命名方式的访问控制列表，以针对不同部门或用户对公司 FTP 服务器不同的网络安全访问的控制。如果配置 ACL 的规则比较多，则应该使用基于名称的访问控制列表来进行管理，这样可以减轻很多后期维护的工作，方便网络管理员随时调整 ACL 规则。

实训 3 网络地址转换

网络地址转换（Network Address Translation, NAT）的功能是将企业内部自行定义的私有 IP 地址转换为 Internet 上可识别的合法 IP 地址。由于现行 IP 地址标准——IPv4 的限制，Internet 面临着 IP 地址空间短缺的问题，从 ISP 申请并给企业的每位员工分配一个合法 IP 地址是不现实的。NAT 技术能较好地解决现阶段 IPv4 地址短缺问题。本实训分为以下两个任务进行学习。

任务 1 利用动态 NAPT 实现局域网访问 Internet。

任务 2 利用 NAT 实现外网主机访问内网服务器。

任务 1 利用动态 NAPT 实现局域网访问 Internet

园区网内通常情况下有很多台主机，从 ISP 申请并给园区网中的每台主机分配一个合法 IP 地址是不现实的，为了使所有内部主机都可以连接到 Internet，需要使用网络地址转换。此外，网络地址转换技术还可以有效地隐藏内部局域网中的主机，具有一定的网络安全保护作用。

学习情境

海成公司由于业务的需要，公司办公网络需要接入 Internet，网络管理员向网络运营商申请了一条专线，该专线分配了一个公网 IP 地址。要求公司所有部门主机都能访问外网。

情境分析

公司通过路由器与外网互连，并且只申请到一个公网地址，即与公网直连的路由器端口的 IP 地址。传统的 NAT 一般是指一对一的地址映射，不能同时满足所有内部网络主机与外部网络通信的需要，而 NAPT 可将网络地址转换后，使多个本地 IP 地址对应一个或多个全局 IP 地址。采用动态的网络端口地址转换（Network Address Port Translation, NAPT）可实现局域网多台主机共用一个或少数几个公网 IP 地址来访问互联网。

所需设备：

(1) Cisco 2911 路由器 2 台。

(2) Cisco-HWIC-2T 高速同步串行模块 2 个。



- (3) Cisco 3560 交换机 1 台。
- (4) Cisco Catalyst 2960 交换机 2 台。
- (5) DCE 串口和 DTE 串口线 1 条。
- (6) 直通线 3 条。
- (7) 交叉线 2 条。
- (8) PC 2 台，服务器 1 台。
- (9) Console 线 1 条。

任务拓扑结构如图 5-3-1-1 所示。

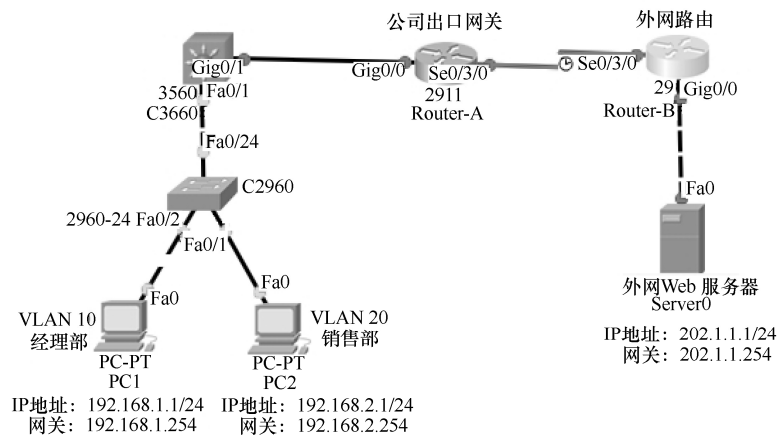


图 5-3-1 利用动态 NAPT 实现局域网访问 Internet

网络设备、PC 的 IP 地址及端口信息，如表 5-3-1 所示。

表 5-3-1 网络设备、PC 的 IP 地址及端口信息表

设 备	接 口	IP 地址	子 网 掩 码	默 认 网 关
Router-A	G0/0	192.168.10.1	255.255.255.0	
	S0/3/0	201.1.8.1	255.255.255.0	
Router-B	G0/0	202.1.1.254	255.255.255.0	
	S0/3/0 (DCE)	201.1.8.10	255.255.255.0	
C3560	VLAN 10	192.168.1.254	255.255.255.0	
	VLAN 20	192.168.2.254	255.255.255.0	
	G0/1	192.168.10.2	255.255.255.0	
PC 1		192.168.1.1	255.255.255.0	192.168.1.254
PC 2		192.168.2.1	255.255.255.0	192.168.2.254
Web 服务器		202.1.1.1	255.255.255.0	202.1.1.254

步骤实现

- 步骤 1：按照图 5-3-1 连接网络拓扑结构。
- 步骤 2：按照表 5-3-1 配置计算机和服务器的 IP 地址、子网掩码和网关。
- 步骤 3：配置路由器 A 的主机名称及其接口 IP 地址。

```
Router>enable
Router#conf t
```

```

Router(config)#hostname Router-A
Router-A(config)#int g0/0
Router-A(config-if)#ip address 192.168.10.1 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config)#int s0/3/0
Router-A(config-if)#ip address 201.1.8.1 255.255.255.0
Router-A(config-if)#no shutdown
Router-A(config-if)#

```

步骤 4: 配置路由器 B 的主机名称及其接口 IP 地址。

```

Router>enable
Router#conf t
Router(config)#hostname Router-B
Router-B(config)#int s0/3/0
Router-B(config-if)#clock rate 64000      ! 设置 DCE 设备端口的时钟频率
Router-B(config-if)#ip address 201.1.8.10 255.255.255.0
Router-B(config-if)#no shutdown
Router-B(config)#int g0/0
Router-B(config-if)#ip add 202.1.1.254 255.255.255.0
Router-B(config-if)#no shutdown
Router-B(config-if)#

```

步骤 5: 配置交换机 C3560 的主机名称和接口 IP 地址。

```

Switch>enable
Switch#conf t
Switch(config)#hostname C3560
Switch(config)#ip routing
C3560(config)#int g0/1
C3560(config-if)#no switchport      ! 将交换端口转换为物理端口
C3560(config-if)#ip add 192.168.10.2 255.255.255.0      ! 配置交换机物理端口的 IP 地址
C3560(config-if)#no shutdown
C3560(config-if)#exit

```

步骤 6: 配置交换机 C2960 的主机名称, 创建 VLAN 10 和 VLAN 20, 将 Fa0/1 划入 VLAN 10, Fa0/2 划入 VLAN 20。

```

Switch(config)#hostname C2960
C2960(config)#vlan 10
C2960(config-vlan)#exit
C2960(config)#vlan 20
C2960(config-vlan)#exit
C2960(config)#int f0/1
C2960(config-if)#switchport mode access
C2960(config-if)#switchport access vlan 10
C2960(config)#int f0/2
C2960(config-if)#switchport mode access
C2960(config-if)#switchport access vlan 20
C2960(config-if)#

```



步骤 7：在交换机 C3560 上创建 VLAN、配置中继链路，设置 SVI 接口的 IP 地址。

```
C3560(config)#vlan 10
C3560(config-vlan)#exit
C3560(config)#vlan 20
C3560(config-vlan)#exit
C3560(config)#int f0/1
C3560(config-if)#switchport mode trunk
C3560(config-if)#exit
C3560(config)#int vlan 10
C3560(config-if)#ip address 192.168.1.254 255.255.255.0
C3560(config-if)#no shutdown
C3560(config)#int vlan 20
C3560(config-if)#ip address 192.168.2.254 255.255.255.0
C3560(config-if)#no shutdown
C3560(config-if)#
```

步骤 8：在交换机 C3560 和路由器 A 上配置路由，实现各部门与公司网络出口的链路通信。

```
C3560(config)#ip route 0.0.0.0 0.0.0.0 192.168.10.1
Router-A(config)#ip route 192.168.1.0 255.255.255.0 192.168.10.2
Router-A(config)#ip route 192.168.2.0 255.255.255.0 192.168.10.2
```

步骤 9：在路由器 A 上配置默认路由，实现外网可达。

```
Router-A(config)#ip route 0.0.0.0 0.0.0.0 201.1.8.10
```

步骤 10：在路由器 A 上配置动态 NAT，使公司内网用户可以访问外网 Web 服务器。

```
Router-A(config)#access-list 10 permit 192.168.0.0 0.0.255.255
! 配置访问控制列表，定义需要通过地址转换访问外网的用户

Router-A(config)#ip nat pool to_internet 201.1.8.1 201.1.8.1 netmask
255.255.255.0 ! 定义 NAT 地址池

Router-A(config)#ip nat inside source list 10 pool to_internet overload
! 配置动态 NAT，实现地址转换

Router-A(config)#int s0/3/0 ! 进入出口路由器的外网接口
Router-A(config-if)#ip nat outside ! 定义 NAT 的外网接口

Router-A(config-if)#exit
Router-A(config)#int g0/0 ! 进入出口路由器的内网接口
Router-A(config-if)#ip nat inside ! 定义 NAT 的内网接口

Router-A(config-if)#exit
Router-A(config)#
```



小贴士

在出口路由器上需要正确设置 NAT 的内网接口和外网接口。

在配置内网通信时需要添加能使内网数据包向外转发的路由，如默认路由等。

在内网用户较多的情况下，尽量不要使用广域网接口地址作为映射的全局地址，因为路由器支持的 PAT 会话是有限制的。此例中仅有一个公网 IP 地址。

步骤 11：测试内网用户能否访问外网 Web 服务器，如图 5-3-2 所示。

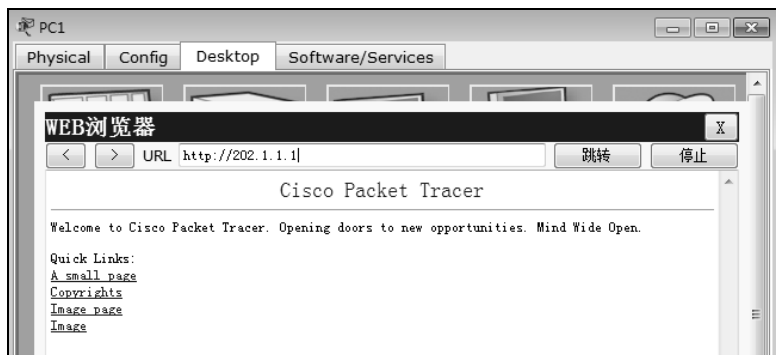


图 5-3-2 内网用户访问外网 Web 服务器

步骤 12: 查看 NAT 配置信息。

(1) 查看 NAT 映射表。

```
Router-A#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 201.1.8.1:1025 192.168.1.1:1025 202.1.1.1:80 202.1.1.1:80
Router-A#
```

(2) 查看 NAT 信息统计表。

```
Router-A#show ip nat statistics
Total translations: 1 (0 static, 1 dynamic, 1 extended)
Outside Interfaces: Serial0/3/0
Inside Interfaces: GigabitEthernet0/0
Hits: 8 Misses: 1
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 10 pool to_internet refCount 1
pool to_internet: netmask 255.255.255.0
start 201.1.8.1 end 201.1.8.1
type generic, total addresses 1 , allocated 1 (100%), misses 0
Router-A#
```

相关知识

1. NAT

目前互联网的一个重要问题是 IP 地址需求急剧膨胀, IP 地址空间衰竭, NAT 的使用从一定程度上缓解了该问题。NAT 的使用, 使得一个组织内部的私有 IP 地址转换为可以在互联网上通信的公有 IP 地址, 从而实现了组织内部网络与互联网的连接, 而不需要重新给组织内部网络中的每台主机分配公有 IP 地址。

NAT 的优点如下。

(1) 节省 IP 资源, 从一定程度上解决了 IP 地址短缺问题。

(2) 可以实现服务器 TCP 负载均衡, 维持 TCP 会话。

(3) 连接地址池中的 IP 地址可以是虚拟 IP 地址, 不一定需要配置在物理接口上, 这样维护起来比较方便。



(4) 可以解决地址重叠问题。

NAT 的缺点如下。

(1) 增加了传输延迟。

(2) 隐藏了端对端的 IP 地址，不利于某些程序的应用。

(3) 不便于跟踪、管理。

2. NAT 的工作过程

(1) 客户机将数据包发给运行 NAT 的计算机上。

(2) NAT 将数据包中的端口号和专用的 IP 地址换成自己的端口号和公用的 IP 地址，然后将数据包发送给外部网络的目的主机，同时在映像表中记录跟踪信息，以便向客户机发送回答信息。

(3) 外部网络发送回答信息给 NAT。

(4) NAT 将收到的数据包的端口号和公用 IP 地址转换为客户机的端口号和内部网络使用的专用 IP 地址，并转发给客户机。

3. NAT 的配置

1) 静态 NAT

静态 NAT 将内部地址和外部地址进行一对一的转换。这种方法要求申请到的合法 IP 地址足多多，可以与内部 IP 地址一一对应。

静态 NAT 一般用于那些需要固定的合法 IP 地址的主机，如 Web 服务器、FTP 服务器、E-mail 服务器等，如图 5-3-3 所示。

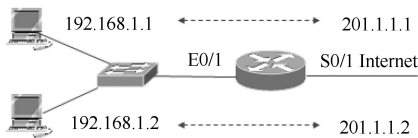


图 5-3-3 静态 NAT

其配置步骤如下。

(1) 定义内部源地址静态转换关系：

```
Router(config)# ip nat inside source static local-address global-address
```

(2) 定义接口连接内部网络：

```
Router(config)# ip nat inside
```

(3) 定义接口连接外部网络：

```
Router(config)# ip nat outside
```

示例：

```
Router(config)# ip nat inside source static 192.168.1.1 201.1.1.1
Router(config)# int e0/1
Router(config-if)# in nat inside
Router(config)# int s0/1
Router(config-if)# in nat outside
```

2) 动态 NAT

动态 NAT 将多个合法 IP 地址统一地组织起来，构成一个 IP 地址池，当有主机需要访问外网时，分配一个合法 IP 地址与内部地址进行转换，当主机使用结束后，归还该地址。对于

NAT 池，如果同时联网用户太多，则可能出现地址耗尽的问题，如图 5-3-4 所示。

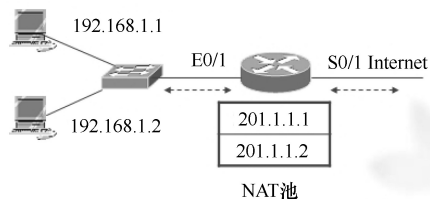


图 5-3-4 动态 NAT

其配置步骤如下。

(1) 定义全局 IP 地址池：

```
Router(config)# ip nat pool address-pool start-address end-address {network mask | prefix-length prefix-length }
```

(2) 定义访问控制列表，只有匹配该列表的地址才能转换：

```
Router(config)# access-list access-list-number permit ip-address wildcard
```

(3) 定义内部源地址动态转换关系：

```
Router(config)# ip nat inside source list access-list-number pool address-pool
```

(4) 定义接口连接内部网络：

```
Router(config)# ip nat inside
```

(5) 定义接口连接外部网络：

```
Router(config)# ip nat outside
```

示例：

```
Router(config)# ip nat pool to_internet 201.1.1.1 201.1.1.2 netmask 255.255.255.0
Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 10 pool to_internet
Router(config)# int e0/1
Router(config-if)# ip nat inside
Router(config)# int s0/1
Router(config-if)# ip nat outside
```

3) PAT

使用端口多路复用技术，将多个内部地址映射为一个合法地址，用不同的端口号区分各个内部地址。这种方法只需要一个合法 IP 地址。路由器支持的 PAT 会话数是有限制的，所以使用 PAT 的局域网，其网络的规模不能太大。

在端口复用技术中，用端口区分的不是主机，而是一个会话（网络连接），当一台主机同时建立多个会话时，它的每个会话会占用一个端口映射。理论上讲，一个 IP 地址可以映射约 65000 个会话，但实际的路由器往往只支持几千个会话（Cisco 支持约 4000 个会话），如图 5-3-5 所示。

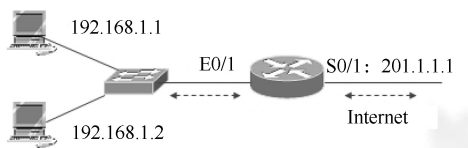


图 5-3-5 PAT



其配置步骤如下。

(1) 定义访问控制列表，只有匹配该列表的地址才能转换：

```
Router(config)# access-list access-list-number permit ip-address wildcard
```

(2) 定义内部源地址复用转换关系：

```
Router(config)# ip nat inside source list access-list-number interface interface-number overload
```

(3) 定义接口连接内部网络：

```
Router(config)# ip nat inside
```

(4) 定义接口连接外部网络：

```
Router(config)# ip nat outside
```

示例：

```
Router(config)# access-list 10 permit 192.168.1.0 0.0.0.255
Router(config)# ip nat inside source list 10 interface s0/1 overload
Router(config)# int e0/1
Router(config-if)# in nat inside
Router(config)# int s0/1
Router(config-if)# in nat outside
```

课堂训练

某公司的拓扑图如图 5-3-6 所示。R1 是局域网的边界路由器，R2 是 ISP 的路由器，局域网使用私有地址 192.168.1.0/24 进行编址。ISP 为局域网分配了一个合法地址池 200.1.1.2~200.1.1.4/24。路由器端口及主机 IP 地址如表 5-3-2 所示。

通过配置动态 NAPT 实现内网主机访问外网功能。

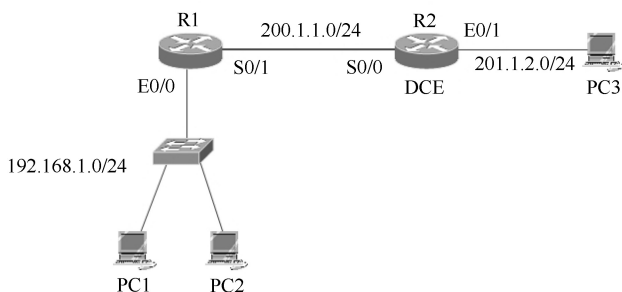


图 5-3-6 某公司拓扑图

表 5-3-2 路由器端口及主机 IP 地址

设 备	接 口	IP 地址
R1	E0/0	192.168.1.254/24
	S0/1	200.1.1.1/24
R2	S0/0	200.1.1.10/24
	E0/1	201.1.2.1/24
PC 1	Fa0	192.168.1.1/24
PC 2	Fa0	192.168.1.2/24
PC 3	Fa0	201.1.2.2/24

学习小结

本任务介绍了使用动态 NAPT 来使内网用户通过网络地址转换来访问 Internet。动态 NAPT 可实现多个内网本地 IP 地址共用一个或少数几个公网 IP 地址来访问互联网，同时每个公网 IP 地址通过端口号来区分内网主机发起的会话，极大地缓解了内网主机数量多而公网 IP 地址短缺的矛盾，在园区网络中应用比较广泛。

任务 2 利用 NAT 实现外网主机访问内网服务器

学习情境

海成公司的办公网络接入了 Internet，由于需要企业宣传，故建立了网站用于产品推广和业务交流。目前，公司只向网络运营商申请了一个公网 IP 地址，服务器位于公司内网中。公司要求内网用户能够访问 Internet，并要求客户在互联网上可以访问公司的内部网站。

情境分析

公司只申请了一个公网 IP 地址，基于私有地址与公有地址不能直接通信的原则，公网的计算机是不能直接访问内网服务器的，要使内网服务器上的服务能够被外网主机访问，就要将内网服务器的私有 IP 地址通过基于 Web 端口的静态转换映射到公网的 IP 地址上，这样互联网上的用户才能通过公网 IP 地址访问到内网服务器。此外，公司内网用户访问互联网可以通过动态 NAPT 来实现。

所需设备：

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco-HWIC-2T 高速同步串行模块 2 个。
- (3) Cisco 3560 交换机 1 台。
- (4) Cisco Catalyst 2960 交换机 2 台。
- (5) DCE 串口和 DTE 串口线 1 条。
- (6) 直通线 4 条。
- (7) 交叉线 2 条。
- (8) PC 3 台，服务器 1 台。
- (9) Console 线 1 条。

任务拓扑结构如图 5-3-7 所示。

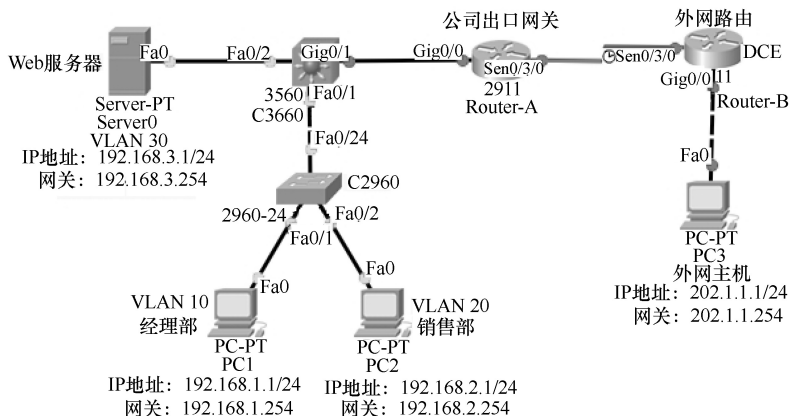


图 5-3-7 利用 NAT 实现外网主机访问内网服务器



网络设备、PC 的 IP 地址及端口信息如表 5-3-3 所示。

表 5-3-3 网络设备、PC 的 IP 地址及端口信息

设 备	接 口	IP 地址	子 网 掩 码	默 认 网 关
Router-A	G0/0	192.168.10.2	255.255.255.0	
	S0/3/0	201.1.1.1	255.255.255.0	
Router-B	S0/3/0 (DCE)	201.1.1.10	255.255.255.0	
	G0/0	202.1.1.254	255.255.255.0	
C3560	G0/1	192.168.10.1	255.255.255.0	
	VLAN 10	192.168.1.254	255.255.255.0	
	VLAN 20	192.168.2.254	255.255.255.0	
	VLAN 30	192.168.3.254	255.255.255.0	
PC 1		192.168.1.1	255.255.255.0	192.168.1.254
PC 2		192.168.2.1	255.255.255.0	192.168.2.254
Web 服务器		192.168.3.1	255.255.255.0	192.168.3.254
外网主机		202.1.1.1	255.255.255.0	202.1.1.254

步骤实现

步骤 1：按照图 5-3-7 连接网络拓扑结构。

步骤 2：按照表 5-3-3 配置计算机和服务器的 IP 地址、子网掩码和网关。

步骤 3：配置路由器 A 的主机名称及其接口 IP 地址。

```
Router>enable
Router#conf t
Router(config)#hostname Router-A
ROUTER-A(config)#int g0/0
ROUTER-A(config-if)#ip address 192.168.10.2 255.255.255.0
ROUTER-A(config-if)#no shutdown
ROUTER-A(config)#int s0/3/0
ROUTER-A(config-if)#ip address 201.1.1.1 255.255.255.0
ROUTER-A(config-if)#no shutdown
ROUTER-A(config-if)#
```

步骤 4：配置路由器 B 的主机名称及其接口 IP 地址。

```
Router>enable
Router#conf t
Router(config)#hostname Router-B
Router-B(config)#int s0/3/0
Router-B(config-if)#clock rate 64000
Router-B(config-if)#ip address 201.1.1.10 255.255.255.0
Router-B(config-if)#no shutdown
Router-B(config)#int g0/0
Router-B(config-if)#ip address 202.1.1.254 255.255.255.0
Router-B(config-if)#no shutdown
Router-B(config-if)#
```

步骤 5: 配置交换机 C3560 的主机名称及其接口 IP 地址。

```
Switch>enable
Switch#conf t
Switch(config)#hostname C3560
Switch(config)#ip routing
C3560(config)#int g0/1
C3560(config-if)#no switchport
C3560(config-if)#ip address 192.168.10.1 255.255.255.0
C3560(config-if)#no shutdown
C3560(config-if)#
```

步骤 6: 配置交换机 C2960 的主机名称, 创建 VLAN 10 和 VLAN 20, 将 Fa0/1 划入 VLAN 10, Fa0/2 划入 VLAN 20。

```
Switch>enable
Switch#conf t
Switch(config)#hostname C2960
C2960(config)#vlan 10
C2960(config-vlan)#exit
C2960(config)#vlan 20
C2960(config-vlan)#exit
C2960(config)#int f0/1
C2960(config-if)#switchport mode access
C2960(config-if)#switchport access vlan 10
C2960(config)#int f0/2
C2960(config-if)#switchport mode access
C2960(config-if)#switchport access vlan 20
C2960(config-if)#
```

步骤 7: 在交换机 C3560 上创建 VLAN, 配置中继链路, 设置 SVI 接口的 IP 地址。

```
C3560(config)#vlan 10
C3560(config-vlan)#exit
C3560(config)#vlan 20
C3560(config-vlan)#exit
C3560(config)#vlan 30
C3560(config-vlan)#exit
C3560(config)#int f0/2
C3560(config-if)#switchport mode access
C3560(config-if)#switchport access vlan 30
C3560(config)#int f0/1
C3560(config-if)#switchport mode trunk
C3560(config)#int vlan 10
C3560(config-if)#ip address 192.168.1.254 255.255.255.0
C3560(config-if)#no shutdown
C3560(config)#int vlan 20
```



```
C3560(config-if)#ip address 192.168.2.254 255.255.255.0
C3560(config-if)#no shutdown
C3560(config)#int vlan 30
C3560(config-if)#ip address 192.168.3.254 255.255.255.0
C3560(config-if)#no shutdown
C3560(config-if)#
```

步骤 8：在交换机 C3560 上配置 RIPv2 动态路由协议，实现各部门与公司网络出口的链路通信。

```
C3560(config)#router rip
C3560(config-router)#version 2
C3560(config-router)#no auto-summary
C3560(config-router)#network 192.168.1.0
C3560(config-router)#network 192.168.2.0
C3560(config-router)#network 192.168.3.0
C3560(config-router)#network 192.168.10.0
C3560(config-router)#exit
```

步骤 9：在路由器 A 上配置 RIPv2 动态路由协议，实现各部门与公司网络出口的链路通信。

```
ROUTER-A(config)#router rip
ROUTER-A(config-router)#version 2
Router-A(config-router)#no auto-summary
Router-A(config-router)#network 192.168.10.0
Router-A(config-router)#default-information originate ! 重分布默认路由
Router-A(config-router)#exit
Router-A(config)#ip route 0.0.0.0 0.0.0.0 201.1.1.10
```

步骤 10：在路由器 A 上配置动态 NAT，使公司内网部门用户可以访问外网。

```
Router-A(config)#access-list 10 permit 192.168.1.0 0.0.0.255
Router-A(config)#access-list 10 permit 192.168.2.0 0.0.0.255
! 配置访问控制列表，定义需要访问外网的用户网段
Router-A(config)#ip nat pool to_internet 201.1.1.1 201.1.1.1 netmask
255.255.255.0
Router-A(config)#ip nat inside source list 10 pool to_internet overload
Router-A(config)#int s0/3/0
Router-A(config-if)#ip nat outside
Router-A(config-if)#exit
Router-A(config)#int g0/0
Router-A(config-if)#ip nat inside
Router-A(config-if)#exit
```



小贴士

为了尽可能地保护内网服务器的安全，服务器一般不会将所有服务都映射到公网 IP 地址上。因此，在本例中，服务器网段不会加入到需要动态 NAT 映射的内网地址段中。

步骤 10：配置基于端口的静态地址映射，使外网用户能访问内网 Web 服务器。

```
Router-A(config)#ip nat inside source static tcp 192.168.3.1 80 201.1.1.1 80
! 配置基于 80 端口（Web 服务）的静态地址映射
```

步骤 11：测试外网主机访问内网 Web 服务，发现可以访问，如图 5-3-8 所示。

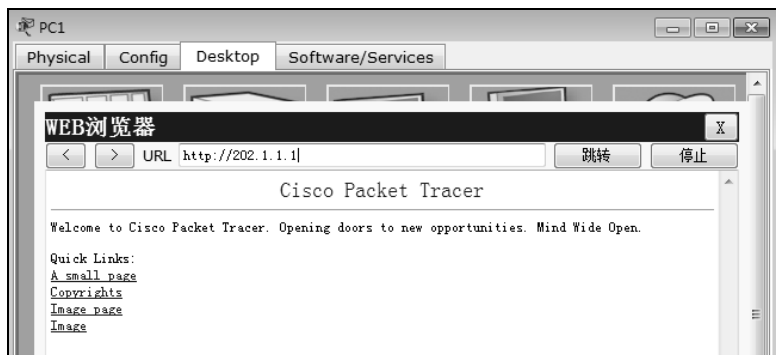


图 5-3-8 外网主机访问内网 Web 服务

步骤 12: 查看 NAT 配置信息。

(1) 查看 NAT 映射表。

```
Router-A#show ip nat t
Router-A#show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 201.1.1.1:80 192.168.3.1:80 --- ---
Router-A#
```

(2) 查看 NAT 信息统计表。

```
Router-A#show ip nat statistics
Total translations: 1 (1 static, 0 dynamic, 1 extended)
Outside Interfaces: Serial0/3/0
Inside Interfaces: GigabitEthernet0/0
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 10 pool to_internet refCount 0
pool to_internet: netmask 255.255.255.0
start 201.1.1.1 end 201.1.1.1
type generic, total addresses 1 , allocated 0 (0%), misses 0
Router-A#
```

相关知识

1. 静态 NAT

基于端口的静态地址映射即静态 NAT。传统的 NAT 一般是指一对一的地址映射，不能同时满足所有内部网络主机与外部网络通信的需要。使用 NAT，可以将多个内部本地地址映射到一个内部全局地址上。

NAT 分为静态 NAT 和动态 NAT。静态 NAT 一般应用在于将内部网指定主机的指定端口映射到全局地址的指定端口上。而静态 NAT 则将内部主机映射为全局地址，显然不可能提供那么多的全局地址。

2. 静态 NAT 配置

(1) 定义内部源地址静态转换关系，即基于端口的静态映射：

```
Router(config)# ip nat inside source static {UDP | TCP} local-address port
global-address port
```




(2) 定义接口连接内部网络:

```
Router(config)# ip nat inside
```

(3) 定义接口连接外部网络:

```
Router(config)# ip nat outside
```

示例:

```
Router(config)# ip nat inside source static tcp 192.168.1.1 80 201.1.1.1 80
```

! 将内网 IP 地址为 192.168.1.1 的主机的 Web 服务静态映射到公网 IP 地址 (201.1.1.1) 上

```
Router(config)# int e0/1
```

```
Router(config-if)# in nat inside
```

```
Router(config)# int s0/1
```

```
Router(config-if)# in nat outside
```

课堂训练

(1) 静态 NAT 配置练习: 将一台内网的 Web 服务器 (IP 地址为 192.168.12.3) 映射到全局 IP 地址 (200.198.12.1) 的 80 端口上。

(2) 静态 NAT 配置练习: 将一台内网主机 (IP:192.168.10.1) 的远程连接功能映射到全局 IP 地址 (198.101.1.1) 的 23 端口上。

学习小结

本任务介绍了配置基于端口的静态地址映射 (静态 NAT) 来实现外网用户访问内网 Web 服务。针对园区网中服务器只向外网提供部分应用服务的情况, 一般会采用静态 NAT 来实现, 这样既可以在一定程度上保护内网服务器, 又可以尽可能地节约公网 IP 地址。

项目考核

(1) 海成公司组建了园区网络, 如图 5-3-9 所示。其有行政部、财务部、职工宿舍、销售部和网管中心 5 个部门, 行政部、财务部、职工宿舍及网管中心通过公司的核心交换机进行连接, 实现数据交换; 销售部通过一条专线直接连接到出口路由器上。公司核心交换机与出口路由器直接相连, 实现公司各部门之间的通信。同时, 公司向 ISP 申请了一组公网 IP 地址, 用于实现公司用户访问 Internet。网络设备、PC 的 IP 地址信息如表 5-3-4 所示。

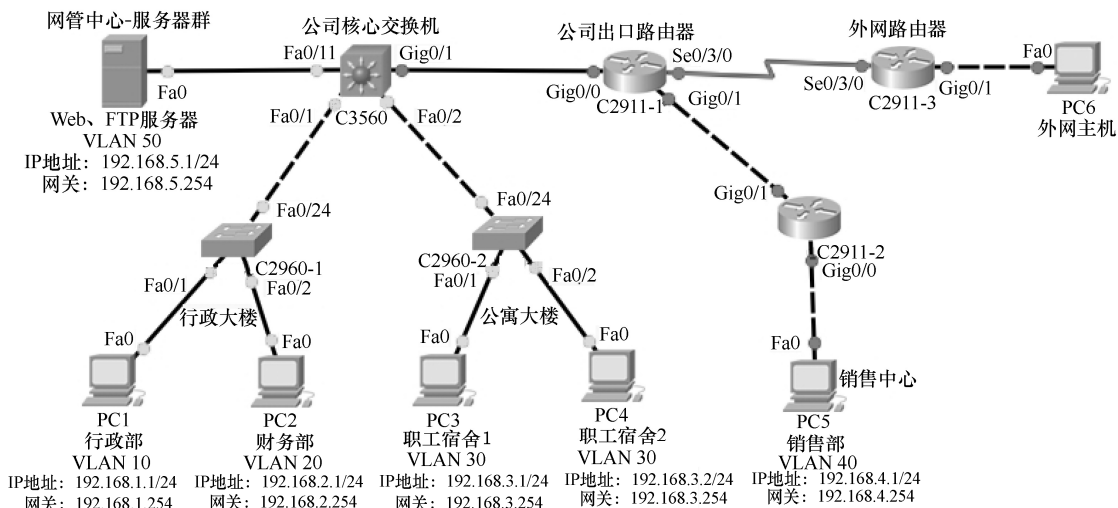


图 5-3-9 海成公司拓扑结构图

要求实现以下功能。

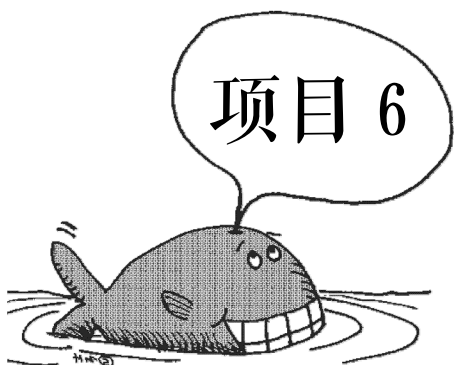
- ① 部署公司内部的网络安全，保障工作网络正常运行，强化对公司内网的管理。
- ② 内网用户能够正常访问互联网。
- ③ 向外网用户提供公司的网站服务，尽可能地保障内网服务器的安全。

表 5-3-4 网络设备、PC 的 IP 地址信息

设 备	接 口	IP 地址	默 认 网 关
Router-A	G0/0	192.168.10.2/24	
	G0/1	192.168.11.2/24	
	S0/3/0 (DCE)	201.1.1.1/24	
Router-B	G0/1	192.168.11.1/24	
	G0/0	192.168.4.254/24	
C2911-3	S0/3/0	201.1.1.100/24	
	G0/1	200.1.1.254/24	
C3560	G0/1	192.168.10.1/24	
	VLAN 10	192.168.1.254/24	
	VLAN 20	192.168.2.254/24	
	VLAN 30	192.168.3.254/24	
	VLAN 50	192.168.5.254/24	
服务器	Fa0	192.168.5.1/24	192.168.5.254
外网主机	Fa0	200.1.1.1/24	200.1.1.254

(2) 海成公司的网络拓扑如图 5-3-9 所示。要求实现下列功能。

- ① 实现公司内网通信及内网用户访问外网的链路可达。
- ② 在公司内网所有接入交换机上配置端口安全功能，要求设置端口的最大连接数为 1，违例处理方式为 restrict。同时，为了减轻网络建设初期时端口与 MAC 地址绑定的工作，要求配置基于粘性的安全 MAC 地址功能。
- ③ 在核心交换机上配置端口安全功能，要求设置服务器 MAC 地址与端口绑定，违例处理方式为 shutdown。
- ④ 部署内网部门间的访问控制，要求网管中心服务器只向用户提供 Web 服务和 FTP 服务，其中，FTP 服务只响应行政部主机的访问，对服务器的所有访问流量均被阻止。
- ⑤ 公司申请了公网 IP 地址池（201.1.1.2/24~201.1.1.5/24）。配置动态 NAT 实现内网用户通过公网 IP 地址池（201.1.1.2/24~201.1.1.4/24）访问互联网。
- ⑥ 配置基于端口的静态地址映射，实现外网用户通过公网 IP 地址 201.1.1.5/24 的 80 端口来访问内网的 Web 服务。



广域网技术实现

项目学习说明

广域网（Wide Area Network, WAN）也称远程网，是一种运行的地域超过局域网的数据通信网络，通常跨接很大的物理范围，所覆盖的范围从几十千米到几千千米，它能连接多个城市或国家，或者横跨几个大洲并能提供远距离通信，形成国际性的远程网络。广域网和局域网的主要区别之一是需要向外部的广域网服务提供商申请订购广域网电信网络服务，一般使用电信运营商提供的数据链路在广域网范围内访问网络。

本项目主要学习 HDLC 协议、PPP 的封装配置，重点学习 PPP 封装 PAP 验证和 PPP 封装 CHAP 验证。

学习能力目标

实训 1：路由器的广域网协议配置。

实训 2：路由器的广域网 PPP 封装验证。

职业能力目标

了解广域网的相关概念和常识。

熟练掌握 HDLC 协议封装的配置方法和步骤。

熟练掌握 PPP 封装的配置方法和步骤。

掌握 PPP 封装 PAP 验证的配置方法和验证。

掌握 PPP 封装 CHAP 验证的配置方法和验证。

理解 PAP 验证的基本过程。

理解 CHAP 验证的优越性。

实训 1 路由器的广域网协议配置

广域网常用数据链路层协议有高级数据链路控制（High-level Data Link Control, HDLC）协议和点到点协议（Point to Point Protocol, PPP）。这些协议定义了数据帧的封装、传输和控制。本实训分为以下两个任务进行学习。

任务 1 路由器的广域网 HDLC 封装。

任务 2 路由器的广域网 PPP 封装。

任务 1 路由器的广域网 HDLC 封装

HDLC 协议是一种标准的用于在同步网络传输数据的、面向比特的数据链路层协议。该协议具有无差错数据传输和流量控制两种功能。作为面向比特的同步通信协议，HDLC 支持全双工点对点的透明传输，支持对等链路。

学习情境

海成公司成功搭建了总公司和分公司的局域网，并运行良好。现购置了两台路由器和高速同步串行模块，准备通过专线将总公司和分公司连接起来，以方便公司内部数据的通信。

情境分析

将两台路由器通过高速同步串行模块连接起来，使用 HDLC 协议进行数据封装和传输。该协议提供了无差错的按序数据传输，并提供流量控制、差错检测和恢复功能以保证数据的完整性。

所需设备：

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco-HWIC-2T 高速同步串行模块 2 个。
- (3) Cisco Catalyst 2960 交换机 2 台。
- (4) DCE 串口和 DTE 串口线 1 条。
- (5) 直通线 4 条。
- (6) PC 2 台。
- (7) Console 线 1 条。

任务拓扑结构如图 6-1-1 所示。

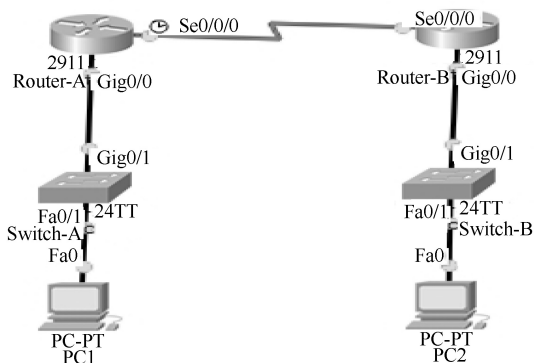


图 6-1-1 广域网 HDLC 协议封装



网络参数设置如表 6-1-1 所示。

表 6-1-1 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Router-A	S0/0/0 (DCE)	202.96.200.1	255.255.255.252	无
	G0/0	192.168.10.1	255.255.255.0	无
Router-B	S0/0/0	202.96.200.2	255.255.255.252	无
	G0/0	192.168.20.1	255.255.255.0	无
PC 1		192.168.10.10	255.255.255.0	192.168.10.1
PC 2		192.168.20.10	255.255.255.0	192.168.20.1

步骤实现

步骤 1：按照图 6-1-1 连接网络拓扑结构。

步骤 2：按照表 6-1-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：路由器 A 的基本配置。

```
Router>enable !进入特权模式
Router#config terminal !进入全局配置模式
Router(config)#hostname Router-A !修改主机名
Router-A(config)#interface gigabitEthernet0/0 !进入接口 G0/0 配置模式
Router-A(config-if)#ip address 192.168.10.1 255.255.255.0
!配置接口 G0/0 的 IP 地址
Router-A(config-if)#no shutdown !启用接口
Router-A(config)#interface serial 0/0/0 !进入接口 S0/0/0 配置模式
Router-A(config-if)#clock rate 800000 !设置 DCE 端同步时钟频率
Router-A(config-if)#ip address 202.96.200.1 255.255.255.252
!配置接口 S0/0/0 的 IP 地址
Router-A(config-if)#no shutdown !启用接口
Router-A(config-if)#
```

步骤 4：路由器 B 的基本配置。

```
Router>enable !进入特权模式
Router#config terminal !进入全局配置模式
Router(config)#hostname Router-B !修改主机名
Router-B(config)#interface gigabitEthernet 0/0 !进入接口 G0/0 配置模式
Router-B(config-if)#ip address 192.168.20.1 255.255.255.0
!配置接口 G0/0 的 IP 地址
Router-B(config-if)#no shutdown !启用接口
Router-B(config)#interface serial0/0/0 !进入接口 S0/0/0 配置模式
Router-B(config-if)#ip address 202.96.200.2 255.255.255.252
!配置接口 S0/0/0 的 IP 地址
Router-B(config-if)#no shutdown !启用接口
Router-B(config-if)#
```

步骤 5：查看路由器 A 的端口配置情况。

```
Router-A#show interfaces serial0/0/0 !查看接口状态
Serial0/0/0 is up, line protocol is up (connected) !接口和协议状态均为 up
```

```

Hardware is HD64570
Internet address is 202.96.200.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)    ! 查看封装协议
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
Router-A#

```

步骤 6: 查看路由器 B 的端口配置情况。

```

Router-B#show int s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 202.96.200.2/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set, keepalive set (10 sec)    ! 查看封装协议
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles

```



```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
Router-B#
```



小贴士

- (1) 注意查看接口状态，接口和协议都必须是 UP。
- (2) CR-V35FC 所连接的接口为 DCE，CR-V35MT 所连接的接口为 DTE。
- (3) 若协议是 down，则通常是因为封装不匹配，或者 DCE 时钟没有配置。
- (4) 若接口是 down，则通常是因为线缆出现了故障。
- (5) 在实际工作中，DCE 设备通常由服务提供商配置，本任务使用的是模拟环境。

步骤 7：配置路由器的默认路由。

```
Router-A(config)#ip route 0.0.0.0 0.0.0.0 202.96.200.2
Router-B(config)#ip route 0.0.0.0 0.0.0.0 202.96.200.1
```

步骤 8：查看路由器 A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 202.96.200.2 to network 0.0.0.0

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0
202.96.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 202.96.200.0/30 is directly connected, Serial0/0/0
L 202.96.200.1/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 202.96.200.2
Router-A#
```

步骤 9：查看路由器 B 的路由表。

```
Router-B#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

```
Gateway of last resort is 202.96.200.1 to network 0.0.0.0
```

```
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
202.96.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 202.96.200.0/30 is directly connected, Serial0/0/0
L 202.96.200.2/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 202.96.200.1
Router-B#
```

步骤 10: 测试连通性, 如图 6-1-2 所示。

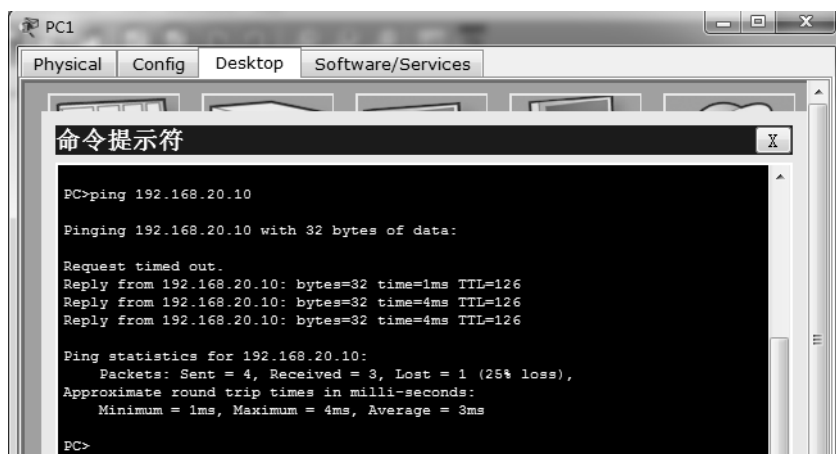


图 6-1-2 连通性测试效果图



小贴士

测试两台计算机之间的连通性, 应本着由近至远的原则。例如, 自 PC 1 测试 PC 2, 应在 PC 1 上依次 ping 以下目标: PC 1 的网关地址、Router A 的 S0/0/0 接口地址、Router B 的 S0/0/0 接口地址、Router A 的 G0/0 接口地址、PC 2 的 IP 地址。这里为了方便, 直接进行了 PC 1 到 PC 2 的测试。

相关知识

1. 广域网

广域网是覆盖多个地区或者国家的计算机网络, 通常由若干个局域网通过电信专用线路连接而成。广域网具有以下特征。

- (1) 覆盖范围广。
- (2) 数据传输速率高。
- (3) 传输延迟大。
- (4) 设备昂贵。

广域网一般只包含 OSI 7 层模型中的下 3 层: 物理层、数据链路层和网络层。广域网一



般采用存储转发方式来进行数据的交换。广域网常用协议如图 6-1-3 所示。



图 6-1-3 广域网常用协议

其中，物理层描述了广域网线路的电气、机械特性；数据链路层描述了数据帧的有序和无差错传输；网络层描述了数据包在局域网之间的路由与转发。

2. HDLC

HDLC 协议起源于 IBM 公司的同步数据链路控制规程（Synchronous Data Link Control, SDLC），后来由 ISO 对其进行扩展修订而来。HDLC 协议是面向比特的在同步网络上进行有序数据传输的数据链路层协议。

HDLC 协议具有以下特征。

- （1）面向比特，不必依赖任何编码方式。
- （2）全双工通信。
- （3）所有数据帧进行 CRC 校验。
- （4）数据传输和控制分离。

HDLC 协议的数据帧格式如图 6-1-4 所示。

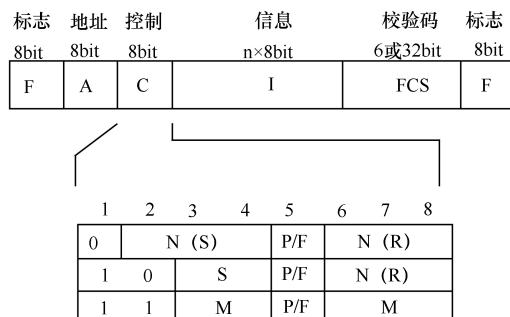


图 6-1-4 HDLC 协议的数据帧格式

HDLC 的数据帧有 3 种类型：信息帧、监控帧、无编号帧。其中，信息帧用于传输有效的数据信息，监控帧用于传输中进行差错控制和流量控制，无编号帧用于对数据链路进行建立、维护和拆除。

由于 HDLC 协议具有较大的自由性、较高的传输效率、较强的传输控制功能，因此，目前网络上大部分设备使用 HDLC 协议作为广域网接口的封装协议。思科公司的路由器广域网接口默认使用 HDLC 协议。

学习小结

本任务介绍了广域网的概念和 HDLC 协议的配置，其中，HDLC 协议是大部分路由器广域网接口的默认协议，可以不用专门配置。值得注意的是，当广域网链路两端的接口使用不同的协议时，是无法通信的。

任务 2 路由器的广域网 PPP 封装

PPP 提供两个对等体之间的数据帧传输，这种传输是有序的、以全双工方式进行的。

与 HDLC 协议相比，PPP 是面向字节的，而 HDLC 协议是面向比特的。PPP 本身也可以工作在面向比特的模式下。

学习情境

海成公司的两台路由器，在实现广域网线路时采用的是默认的 HDLC 协议封装，现公司准备采用目前较为流行的 PPP 来封装广域网线路，希望为公司提供更好的、更安全的网络。

情境分析

两台路由器的广域网端口默认使用了 HDLC 协议来封装，现需要在路由器的广域网端口配置模式下封装 PPP。

所需设备：

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco-HWIC-2T 高速同步串行模块 2 个。
- (3) Cisco Catalyst 2960 交换机 2 台。
- (4) DCE 串口和 DTE 串口线 1 条。
- (5) 直通线 4 条。
- (6) PC 2 台。
- (7) Console 线 1 条。

任务拓扑结构如图 6-1-5 所示。

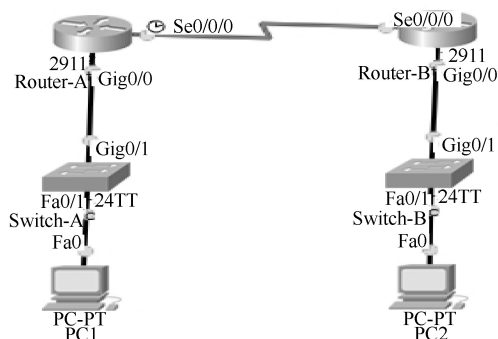


图 6-1-5 路由器的广域网 PPP 封装



网络参数设置如表 6-1-2 所示。

表 6-1-2 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Router-A	S0/0/0 (DCE)	202.96.200.1	255.255.255.252	无
	G0/0	192.168.10.1	255.255.255.0	无
Router-B	S0/0/0	202.96.200.2	255.255.255.252	无
	G0/0	192.168.20.1	255.255.255.0	无
PC 1		192.168.10.10	255.255.255.0	192.168.10.1
PC 2		192.168.20.10	255.255.255.0	192.168.20.1

步骤实现

步骤 1：按照图 6-1-5 连接网络拓扑结构。

步骤 2：按照表 6-1-2 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：路由器 A 的基本配置。

```
Router>enable                                !进入特权模式
Router#config terminal                        !进入全局配置模式
Router(config)#hostname Router-A             !修改主机名
Router-A(config)#interface gigabitEthernet0/0 !进入接口 G0/0 配置模式
Router-A(config-if)#ip address 192.168.10.1 255.255.255.0
!配置接口 G0/0 的 IP 地址
Router-A(config-if)#no shutdown              !启用接口
Router-A(config)#interface serial 0/0/0      !进入接口 S0/0/0 配置模式
Router-A(config-if)#clock rate 800000        !设置 DCE 端的同步时钟频率
Router-A(config-if)#ip address 202.96.200.1 255.255.255.252
Router-A(config-if)#encapsulation ppp        !设置封装协议为 PPP
Router-A(config-if)#no shutdown              !启用接口
!配置接口 S0/0/0 的 IP 地址
Router-A(config-if)#
```

步骤 4：查看路由器 A 的端口配置情况。

```
Router-A#show int s0/0/0
Serial0/0/0 is up, line protocol is down (disabled)
Hardware is HD64570
Internet address is 202.96.200.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Closed
Closed: LEXCP, BRIDGECP, IPCP, CCP, CDPCP, LLC2, BACP
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
```

```
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

DCD=up DSR=up DTR=up RTS=up CTS=up

Router-A#

步骤 5: 路由器 B 的基本配置。

```
Router>enable                                !进入特权模式
Router#config terminal                        !进入全局配置模式
Router(config)#hostname Router-B             !修改主机名
Router-B(config)#interface gigabitEthernet 0/0 !进入接口 G0/0 配置模式
Router-B(config-if)#ip address 192.168.20.1 255.255.255.0
!配置接口 G0/0 的 IP 地址
Router-B(config-if)#no shutdown              !启用接口
Router-B(config)#interface serial0/0/0       !进入接口 S0/0/0 配置模式
Router-B(config-if)#ip address 202.96.200.2 255.255.255.252
!配置接口 S0/0/0 的 IP 地址
Router-B(config-if)#encapsulation ppp        !设置封装协议为 PPP
Router-B(config-if)#no shutdown              !启用接口
```

步骤 6: 再次查看路由器 A 的端口配置情况。

```
Router-A#show int s0/0/0
Serial0/0/0 is up, line protocol is up (connected)
Hardware is HD64570
Internet address is 202.96.200.1/30
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); Total output drops: 0
Queueing strategy: weighted fair
Output queue: 0/1000/64/0 (size/max total/threshold/drops)
```



```
Conversations 0/0/256 (active/max active/max total)
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 packets output, 0 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
DCD=up DSR=up DTR=up RTS=up CTS=up
Router-A#
```



小贴士

广域网链路两端必须使用相同的封装协议，才能够启用数据链路层的连接。在 Cisco Packet Tracer 模拟器中，一个端口的状态如果发生变化，如启用和断开，则模拟器会发送一条提示信息。

步骤 7：配置路由器的默认路由。

```
Router-A(config)#ip route 0.0.0.0 0.0.0.0 202.96.200.2
Router-B(config)#ip route 0.0.0.0 0.0.0.0 202.96.200.1
```

步骤 8：查看路由器 A 的路由表。

```
Router-A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 202.96.200.2 to network 0.0.0.0

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0
202.96.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 202.96.200.0/30 is directly connected, Serial0/0/0
L 202.96.200.1/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 202.96.200.2
Router-A#
```

步骤 9：查看路由器 B 的路由表。

```
Router-B#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
```

Gateway of last resort is 202.96.200.1 to network 0.0.0.0

```
192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
202.96.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 202.96.200.0/30 is directly connected, Serial0/0/0
L 202.96.200.2/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 202.96.200.1
```

Router-B#

步骤 10: 测试连通性, 如图 6-1-6 所示。

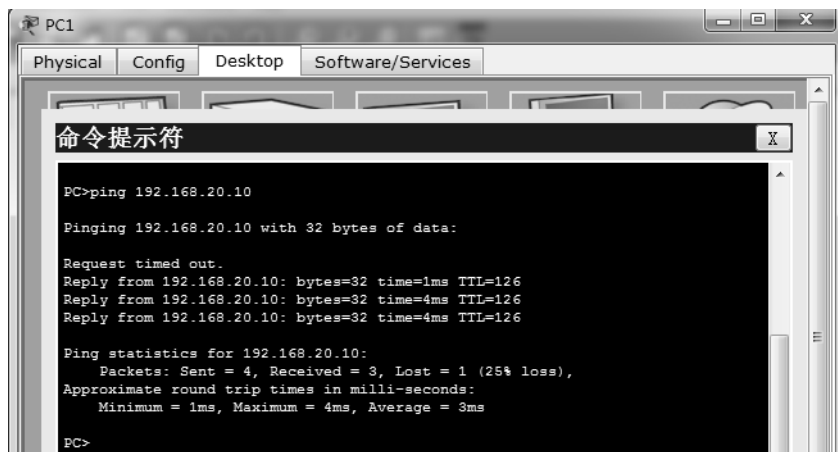


图 6-1-6 连通性测试效果图

小贴士

对于初学者来说, 在实验过程中进行及时的、合理的测试工作非常重要。这有助于学习者尽早地发现问题、准确地定位问题区域, 对于顺利完成整个实验意义重大。

测试工作的一般原则如下。

- (1) 每完成一项设置内容, 都要进行测试或查看。
- (2) 设置完同一条链路两端的地址后, 应及时进行连通性测试。
- (3) 测试较远两个结点的通信, 应本着由近至远的原则, 一个结点接一个结点地进行。

相关知识

PPP 由 Internet IETF 于 1992 年制定, 并于 1993 年和 1994 年分别修订, 最终成为



Internet 的正式标准。

PPP 的前身是串行线路网际协议（Serial Line Internet Protocol, SLIP）。SLIP 在 20 世纪 80 年代曾经广泛应用于 Internet 中，以其简单易用而被称赞。由于 SLIP 只支持一种上层网络协议——IP 协议，并且 SLIP 没有对数据帧的差错检验，因此它有致命的缺陷。PPP 是 TCP/IP 协议栈的标准协议，为同步数据链路的数据传输和控制提供了标准的方法。

PPP 与数据链路层的两个子层——LCP 和 NCP 都有关系。PPP 首先由 LCP 子层发起，主要是建立链路、配置链路参数和测试链路状况等。经过 LCP 子层的初始化工作，由 NCP 来传输上层协议之间的数据通信。

PPP 能够控制数据链路的创建、拆除和维护；支持在数据链路上进行 IP 地址的分配和设置；支持多种类型的网络层协议；可以对数据帧进行差错检验和传输流量控制；链路两端可以就数据压缩的格式进行协商；最为重要的是，在网络安全问题日益严峻的今日，PPP 提供了对广域网的安全保障。

PPP 链路经历的各个阶段，如图 6-1-7 所示。

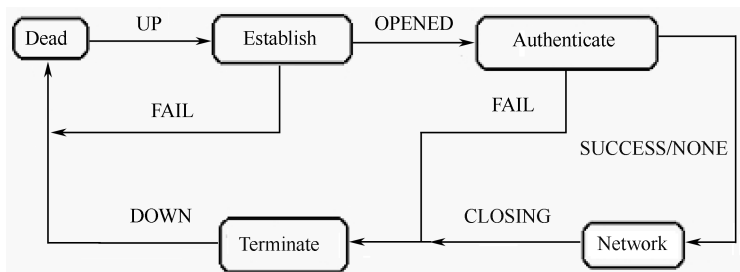


图 6-1-7 PPP 过程状态图

链路不可用阶段（Dead）：PPP 链路需要从此阶段开始，或者以此阶段为终止，当广域网链路激活时，就由此阶段迁移到下一个阶段，即链路建立阶段。

链路建立阶段（Establish）：PPP 在此阶段完成整个协议中最复杂、最关键的工作。PPP 发送配置报文来配置链路参数。如果广域网链路需要进行身份验证，则迁移到验证阶段（Authenticate）；如果链路两端不需要身份验证，则迁移到网络层协议阶段（Network）。

验证阶段：此阶段将对广域网链路的对端进行身份认证。PPP 支持 PAP 和 CHAP 两种认证方式。至于使用哪一种方式，则由链路两端的设备协商决定。默认情况下，不需要进行身份认证。进入这个阶段意味着需要验证对端身份，验证通过后，即可迁移到网络层协议阶段；验证没有通过，则进入网络终止阶段（Terminate）。

网络层协议阶段：PPP 在此阶段对网络层协议进行相应的配置，并在 NCP 的状态为 open 时，封装并传输网络层协议数据信息。当网络层协议数据传输完毕后，进入网络终止阶段。

网络终止阶段：PPP 在此阶段终止链路。链路物理断开、配置参数不匹配、身份认证失败及管理员手工断开链路都会促使链路终止。

学习小结

本实训介绍了广域网链路中的 PPP 封装的配置。路由器进行广域网协议封装时，必须具有相应的广域网功能模块，分辨出线缆的 DCE 和 DTE。路由器两端封装的协议必须一致，否则无法建立链路。

实训 2 路由器的广域网 PPP 封装验证

广域网协议的 PPP 具有密码验证协议（Password Authentication Protocol, PAP）和挑战握手认证协议（Challenge Handshake Authentication Protocol, CHAP）两种验证协议。PAP 认证只在链路建立初期进行，只有两次信息的交换，因此被称为两次握手；CHAP 验证比 PAP 验证更安全。本实训分成为以下两个任务进行。

任务 1 路由器的广域网 PPP 封装 PAP 验证。

任务 2 路由器的广域网 PPP 封装 CHAP 验证。

任务 1 路由器的广域网 PPP 封装 PAP 验证

PAP 验证过程非常简单，验证过程使用明文发送数据包。验证方对验证重试的次数与间隔时间不做要求，皆由被验证方决定。这些都在一定程度上造成了安全隐患。

学习情境

海成公司基于网络安全的考虑，决定在总公司和分公司之间的广域网链路上启用 PAP 验证，以实现总公司路由器对分公司路由器的身份验证。

情境分析

WAN 专线链路建立时要进行安全验证，以保证链路的安全性。链路协商时，PAP 在设备之间传输用户名、密码，以实现用户身份的验证。公司计划在路由器上配置 PPP PAP 认证，以实现链路的安全连接。

所需设备：

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco-HWIC-2T 高速同步串行模块 2 个。
- (3) DCE 串口和 DTE 串口线 1 条。
- (4) 交叉线 2 条。
- (5) PC 2 台。
- (6) Console 线 1 条。

任务拓扑结构如图 6-2-1 所示。

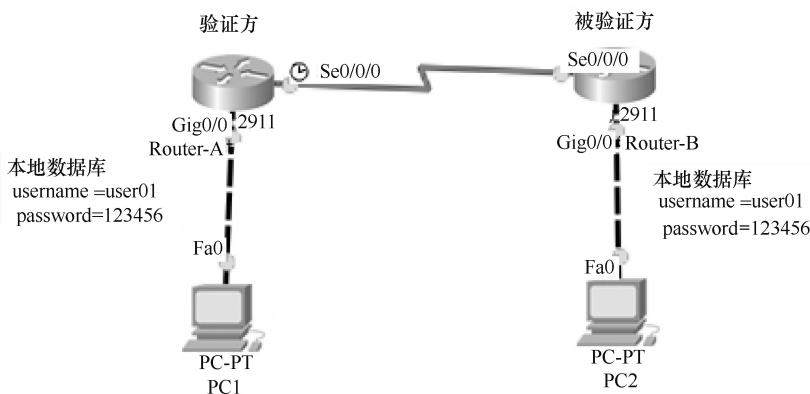


图 6-2-1 海成公司的 PAP 验证拓扑图



网络参数设置如表 6-2-1 所示。

表 6-2-1 网络参数设置

设 备	端 口	IP 地址	子网掩码	网关
Router-A	S0/0/0（DCE）	202.96.200.1	255.255.255.252	无
	G0/0	192.168.10.1	255.255.255.0	无
Router-B	S0/0/0	202.96.200.2	255.255.255.252	无
	G0/0	192.168.20.1	255.255.255.0	无
PC 1		192.168.10.10	255.255.255.0	192.168.10.1
PC 2		192.168.20.10	255.255.255.0	192.168.20.1

步骤实现

步骤 1：按照图 6-2-1 连接网络拓扑结构。

步骤 2：按照表 6-2-1 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：路由器 A 的基本配置。

```
Router>enable                                !进入特权模式
Router#config terminal                        !进入全局配置模式
Router(config)#hostname Router-A!修改主机名
Router-A(config)#interface gigabitEthernet0/0 !进入接口 G0/0 配置模式
Router-A(config-if)#ip address 192.168.10.1 255.255.255.0
!配置接口 G0/0 的 IP 地址
Router-A(config-if)#no shutdown              !启用接口
Router-A(config)#interface serial 0/0/0      !进入接口 S0/0/0 配置模式
Router-A(config-if)#clock rate 800000        !设置 DCE 端的同步时钟频率
Router-A(config-if)#ip address 202.96.200.1 255.255.255.252
!配置接口 S0/0/0 的 IP 地址
Router-A(config-if)#encapsulation ppp        !设置封装协议为 PPP
Router-A(config-if)#no shutdown              !启用接口
Router-A(config-if)#
```

步骤 4：路由器 B 的基本配置。

```
Router>enable                                !进入特权模式
Router#config terminal                        !进入全局配置模式
Router(config)#hostname Router-B             !修改主机名
Router-B(config)#interface gigabitEthernet 0/0 !进入接口 G0/0 配置模式
Router-B(config-if)#ip address 192.168.20.1 255.255.255.0
!配置接口 G0/0 的 IP 地址
Router-B(config-if)#no shutdown!启用接口
Router-B(config)#interface serial0/0/0      !进入接口 S0/0/0 配置模式
Router-B(config-if)#ip address 202.96.200.2 255.255.255.252
!配置接口 S0/0/0 的 IP 地址
Router-B(config-if)#encapsulation ppp        !设置封装协议为 PPP
Router-B(config-if)#no shutdown              !启用接口
Router-B(config-if)#
```

步骤 5：配置路由器的默认路由。

```
Router-A(config)#ip route 0.0.0.0 0.0.0.0 202.96.200.2
```

```
Router-B(config)#ip route 0.0.0.0 0.0.0.0 202.96.200.1
```

步骤 6: 在验证方路由器 A 上创建本地用户数据库。

```
Router-A#conf t      !进入验证方路由器的全局配置模式
```

```
Router-A(config)#username user01 password 123456      !创建本地用户数据库
```

```
Router-A(config)#
```



小贴士

在前面的命令中, username 为用户名, password 为与用户名对应的用户口令。这两项信息应与被验证方的参数一致, 否则无法通过验证过程。

步骤 7: 在验证方路由器 A 上要求进行 PAP 认证。

```
Router-A(config)#int s0/0/0      !进入 S0/0/0 接口配置模式
```

```
Router-A(config-if)#ppp authentication pap      !声明 PAP 认证方式
```

```
Router-A(config-if)#
```



小贴士

在验证方路由器上声明 PAP 认证方式后, 广域网链路 S0/0/0 数据链路层即会断开。这时因为没有在被验证方路由器上进行参数设置, 路由器 B 没有通过路由器 A 的身份认证, 两者之间的数据链路就断开了。

步骤 8: 在被验证方路由器-B 上进行 PAP 客户端参数设置。

```
Router-B(config)#int s0/0/0      !进入被验证方接口配置模式
```

```
Router-B(config-if)#ppp pap sent-username user01 password 123456
```

```
!配置 PAP 客户端的参数信息
```



小贴士

上述命令中 sent-username 后应当输入验证使用的用户名, password 后应当输入该用户对应的用户口令。这两项信息应与验证方路由器 A 上的本地用户数据库的相应信息相同, 否则验证不能通过。

由于路由器 B 通过了路由器 A 的身份认证, 两者之间的链路会重新启用, 路由器 B 的 S0/0/0 数据链路层也改为 UP 模式。

步骤 9: 查看路由器 A 的路由表。

```
Router-A#show ip route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

```
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
* - candidate default, U - per-user static route, o - ODR
```

```
P - periodic downloaded static route
```

```
Gateway of last resort is 202.96.200.2 to network 0.0.0.0
```

```
192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
```

```
C 192.168.10.0/24 is directly connected, GigabitEthernet0/0
```

```
L 192.168.10.1/32 is directly connected, GigabitEthernet0/0
```

```
202.96.200.0/24 is variably subnetted, 2 subnets, 2 masks
```



```
C 202.96.200.0/30 is directly connected, Serial0/0/0
L 202.96.200.1/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 202.96.200.2
Router-A#
```

步骤 10: 查看路由器 B 的路由表。

```
Router-B#showip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 202.96.200.1 to network 0.0.0.0

192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.20.0/24 is directly connected, GigabitEthernet0/0
L 192.168.20.1/32 is directly connected, GigabitEthernet0/0
202.96.200.0/24 is variably subnetted, 2 subnets, 2 masks
C 202.96.200.0/30 is directly connected, Serial0/0/0
L 202.96.200.2/32 is directly connected, Serial0/0/0
S* 0.0.0.0/0 [1/0] via 202.96.200.1
Router-B#
```

步骤 11: 测试。在 PC 1 上 ping PC 2 的 IP 地址 192.168.20.10, 如图 6-2-2 所示。PC 1 能够 ping 通 PC 2, 两台路由器之间可以通信, 说明路由器 A 与路由器 B 之间的 PAP 认证顺利通过了。

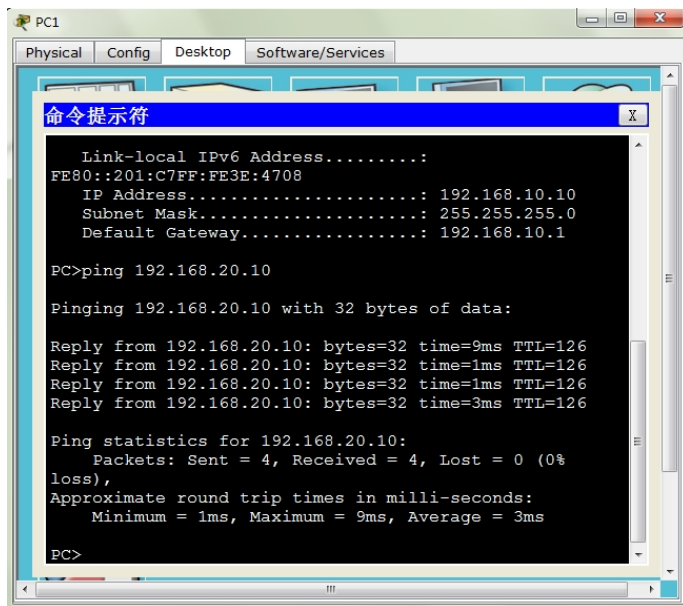


图 6-2-2 连通性测试效果图

相关知识

PAP 是 PPP 中专用于用户身份验证的协议，大部分的路由器都支持这种认证方式。它通过在验证方和被验证方之间的两次握手过程，完成对对端的身份验证。验证过程中，被验证方主动发出验证请求报文，该报文中包含了验证所需的用户名和用户口令。验证方收到请求报文后，将收到的用户名和口令与本地用户数据库中存储的用户名和口令进行对比，如果对比结果相同，则通过验证；否则验证失败。在链路两端的两次握手通信过程中，所使用的报文都是以明文的方式传输的，包括验证所需要的用户名和口令，因此，在 PAP 认证过程中，关键信息很容易被窃取，这为网络安全带来了隐患。

图 6-2-3 描述了 PAP 的验证过程。



图 6-2-3 PAP 验证过程

PAP 工作在数据链路层的 LCP 子层，它通过两次握手的机制来实现对远程对端的身份验证。

PAP 将广域网链路的两端分为验证方和被验证方，验证方通过查看被验证方发送的口令，来确定是否授权创建与对端的连接，从而决定是否进入网络层协议阶段。

学习小结

本任务使用了 PPP 封装路由器广域网并使用 PAP 进行身份验证。读者应学习如何配置本地用户数据库、选择身份认证方式，以及配置 PAP 客户端信息等，学习如何查看路由器配置文件中 PAP 认证的配置信息。

任务 2 路由器的广域网 PPP 封装 CHAP 验证

CHAP 在 LCP 子层通过三次握手来完成对远程链路对端的身份验证。

PAP 的验证过程，需要将用户名与口令以明文的方式通过远程链路传输，这为网络应用带来了安全隐患。CHAP 验证方式在远程链路中只传送用户名而不传送口令，所以在安全性上要比 PAP 高。

CHAP 将远程链路两端分为验证方和被验证方，只用通过了身份认证，才能进入网络层协议阶段。

学习情境

海成公司的管理员发现 PAP 身份验证方式安全性能不高，为了进一步提高网络安全性，决定在总公司和分公司之间的广域网链路上启用 CHAP，以实现总公司路由器对分公司路由器的身份验证。



情境分析

CHAP 使用 3 次握手机制来启动一条链路和周期性的验证远程结点。与 PAP 认证相比，CHAP 认证更具有安全性。CHAP 只在网络上传送用户名而不传送口令，因此安全性更高。

所需设备：

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco-HWIC-2T 高速同步串行模块 2 个。
- (3) DCE 串口和 DTE 串口线 1 条。
- (4) 交叉线 2 条。
- (5) PC 2 台。
- (6) Console 线 1 条。

任务拓扑结构如图 6-2-4 所示。

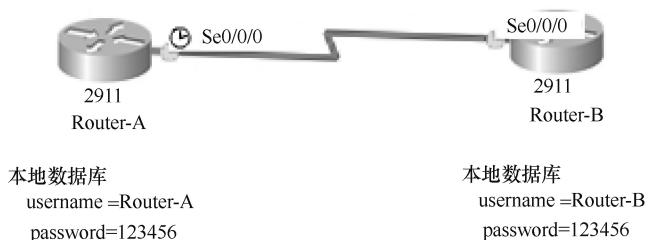


图 6-2-4 海成公司的 CHAP 验证拓扑图

网络参数设置如表 6-2-2 所示。

表 6-2-2 网络参数设置

设备	端口	IP 地址	子网掩码	网关
Router-A	S0/0/0 (DCE)	202.96.200.1	255.255.255.252	无
Router-B	S0/0/0	202.96.200.2	255.255.255.252	无

步骤实现

步骤 1：按照图 6-2-4 连接网络拓扑结构。

步骤 2：按照表 6-2-2 配置计算机的 IP 地址、子网掩码和网关。

步骤 3：路由器 A 的基本配置。

```
Router>enable                                !进入特权模式
Router#config terminal                        !进入全局配置模式
Router(config)#hostname Router-A!修改主机名
Router-A(config)#username Router-B password 123456 !设置用户名及密码
Router-A(config)#interface serial0/0/0      !进入接口 S0/0/0 配置模式
Router-A(config-if)#clock rate 800000       !设置 DCE 端的同步时钟频率
Router-A(config-if)#ip address 202.96.200.1 255.255.255.252
!配置接口 S0/0/0 的 IP 地址
Router-A(config-if)#no shutdown              !启用接口
Router-A(config-if)#
```

步骤 4: 路由器 B 的基本配置。

```
Router>enable                !进入特权模式
Router#config terminal        !进入全局配置模式
Router(config)#hostname Router-B    !修改主机名
Router-B(config)#username Router-A password 123456    !设置用户名及密码
Router-B(config)#interface serial0/0/0    !进入接口 S0/0/0 配置模式
Router-B(config-if)#ip address 202.96.200.2 255.255.255.252
!配置接口 S0/0/0 的 IP 地址
Router-B(config-if)#no shutdown    !启用接口
Router-B(config-if)#
```

步骤 5: 在路由器 A 上封装 PPP, 并进行 CHAP 身份认证。

```
Router-A(config-if)#encapsulation ppp!设置封装协议为 PPP
Router-A(config)#int s0/0/0!进入 S0/0/0 接口配置模式
Router-A(config-if)#ppp authentication chap!声明 CHAP 认证方式
Router-A(config-if)#
```

步骤 6: 在路由器 B 上封装 PPP, 并进行 CHAP 身份认证。

```
Router-B(config-if)#encapsulation ppp!设置封装协议为 PPP
Router-B(config)#int s0/0/0!进入 S0/0/0 接口配置模式
Router-B(config-if)#ppp authentication chap!声明 CHAP 认证方式
Router-B(config-if)#
```



小贴士

在 CHAP 被验证方用户口令数据库中, username 后面的参数应为验证方路由器的 hostname, password 后面为口令参数。验证双方的口令应当完全一样。

步骤 7: 测试。在路由器 A 上 ping 路由器 B 的 IP 地址, 测试结果为两台路由器可以正常通信, 表明 CHAP 验证已通过。

```
Router-A#ping 202.96.200.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.96.200.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms

Router-A#
```

相关知识

CHAP 只在网络链路上传输用户名, 而不会发送用户口令。

验证过程中, 验证方路由器首先向被验证方路由器发送验证请求数据包, 其中包括自己的 hostname (即设备的主机名) 和一段报文, 这段报文是随机产生的。验证方的这种行为被称为挑战。被验证方收到挑战报文后, 读取报文中包含的验证方的主机名, 然后使用此主机名查找本地的本地口令数据库, 找到与验证方主机名对应的用户口令, 使用此用户口令、之前收到的随机报文及报文的 IP 地址, 利用 MD5 算法得到一段应答密文。被验证方路由器随即将该段应答密文连同自己的主机名发送给验证方路由器。验证方收到被验证方发送的应答



报文后，读取其中的被验证方主机名，查找本地口令数据库，找到与被验证方主机名对应的用户口令，使用用户口令、之前产生的随即报文及报文 ID 以 MD5 算法得到一段密文。验证方路由器将这段密文和由被验证方发送的密文进行比较，若二者相同，则认为验证已通过；若二者不同，则验证失败。

图 6-2-5 描述了 CHAP 验证过程。

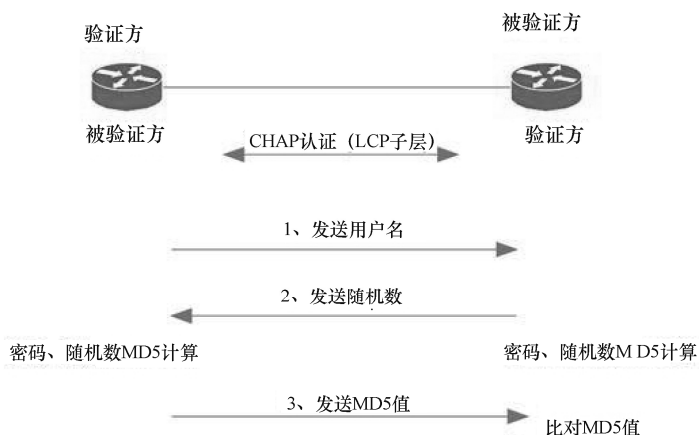


图 6-2-5 CHAP 验证过程

学习小结

本任务介绍了如何使用 PPP 封装广域网并使用 CHAP 进行身份验证。CHAP 采用了 3 次握手机制，比 PAP 具有更高的安全性。在 CHAP 配置中，需要重点注意用户口令数据库的创建，这一点和 PAP 具有本质区别。

项目考核

某公司规模很小，只有一家上海分公司，经理决定组建一个网络实现公司总部和分公司的通信，公司网络管理员经过分析，决定使用 PPP 的 CHAP 认证方式，连接公司总部和分公司，如图 6-2-6 所示，其网络参数设置如表 6-2-3 所示。

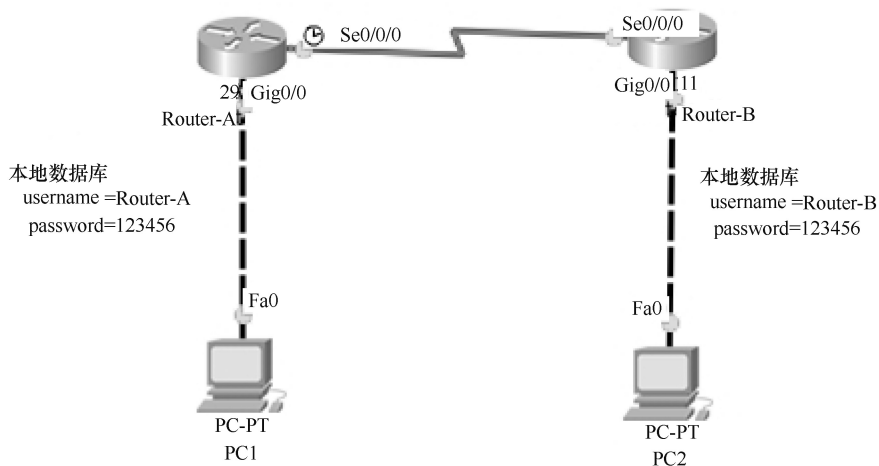
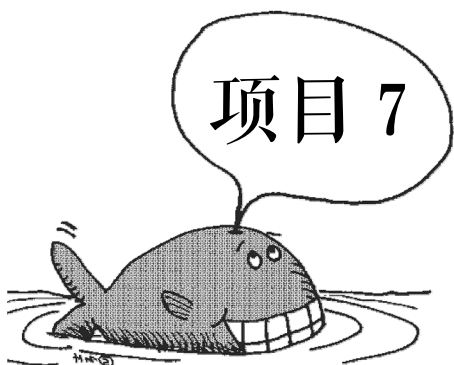


图 6-2-6 某公司的拓扑图

表 6-2-3 网络参数设置

设备	端口	IP 地址	子网掩码	网关
Router-A	S0/0/0 (DCE)	202.96.200.1	255.255.255.252	无
	G0/0	192.168.10.1	255.255.255.0	无
Router-B	S0/0/0	202.96.200.2	255.255.255.252	无
	G0/0	192.168.20.1	255.255.255.0	无
PC 1		192.168.10.10	255.255.255.0	192.168.10.1
PC 2		192.168.20.10	255.255.255.0	192.168.20.1

完成标准：PPP 连接能够正常建立；两个公司的计算机可以相互连通。



无线网络技术实现

项目学习说明

无线网络相对于目前普遍使用的有线网络而言，是一种全新的网络组建方式。无线网络在一定程度上摒弃了有线网络必须依赖的网线，这样，可以坐在家里的任何一个角落，使用笔记本式计算机，享受网络的乐趣，而不像从前那样必须迁就于网络接口的布线位置。

由于无线网络市场热度迅速飙升，已经成为现今 IT 市场中新的增长亮点。无线局域网产品迅速发展并走向成熟，正在以其高速传输功能和灵活性发挥着日益重要的作用，并且无线网络已经开始在国内大多数行业中得到应用。无线网络自问世以来，以其无可比拟的优势迅速深入各行各业。无线网络带来了一种新的上网理念，人们不需要顾虑网线的长短，无线自由联网的特性满足了人们长期以来期望自由上网的愿望。无线网络安装方便，性价比高，成为当今网络发展的趋势所向。

本项目重点学习无线网络的基本配置、无线网络的安全管理和无线网络全网互连。

学习能力目标

实训 1：无线网络的基本配置。

实训 2：无线网络的安全管理。

实训 3：有线和无线网络的全网互连。

职业能力目标

理解无线网络的常用术语。

熟悉无线 AP 的作用和基本配置方法。

熟悉无线网络的基本安全管理技术。

能综合有线、无线路由交换知识实现网络互连互通。

实训 1 无线网络的基本配置

无线接入点（Access Point，AP）也称无线网桥、无线网关。它不仅包含单纯性无线接入点（无线 AP），也同样是无线路由器（含无线网关、无线网桥）等类设备的统称。它主要用于宽带家庭、大楼内部、校园内部、园区内部及仓库、工厂等需要无线监控的地方，典型距离为几十米至上百米，也可以用于远距离传送，目前距离最远可以达到 30km 左右，主要技术为 IEEE 802.11 系列。

学习情境

海成公司由于规模的扩大，在原有网络的基础上，购置了几台无线网络设备和终端，准备搭建自己的无线局域网，满足移动办公的需要。

情境分析

规划与实施该公司的项目时，要认真分析无线设备的技术、了解无线 AP 的功能和基本设置方法，熟悉架设无线网络的基本方法和流程。

所需设备：

- (1) Cisco WRT300N 无线路由器 2 台。
- (2) Cisco Catalyst 2960 交换机 1 台。
- (3) Web 服务器 1 台。
- (4) 用户移动终端 3 台。
- (5) 直通线 3 条。
- (6) Console 线 1 条。

实训拓扑结构如图 7-1-1 所示。

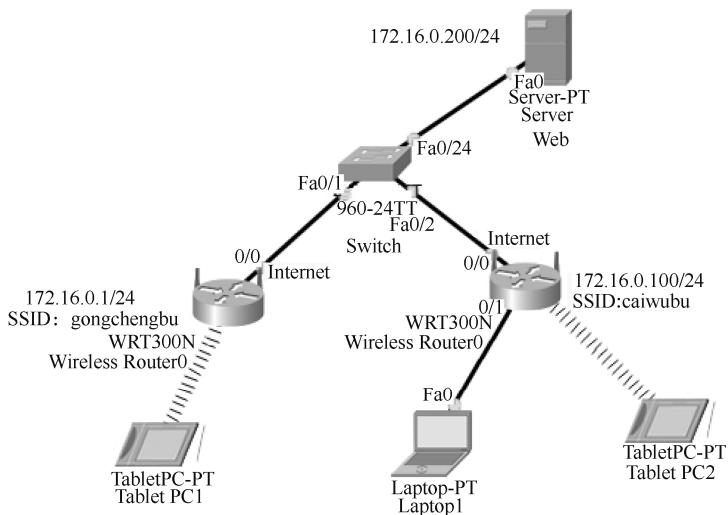


图 7-1-1 海成公司网络拓扑图

无线设备的 IP 地址和 SSID 分配情况如表 7-1-1 所示。



表 7-1-1 无线设备的 IP 地址和 SSID 分配表

名 称	IP 地址	子 网 掩 码	SSID
Wireless Router0	172.16.0.1	255.255.255.0	gongchengbu
Wireless Router1	172.16.0.100	255.255.255.0	caiwubu
Web 服务器	172.16.0.200	255.255.255.0	
Laptop1	自动获取		
Tablet PC1	自动获取		

步骤实现

步骤 1：按照图 7-1-1 连接网络拓扑结构。

步骤 2：按照表 7-1-1 配置移动终端和服务器的 IP 地址、子网掩码。

步骤 3：登录无线路由器 Wireless Router1。

单击 Laptop1，选择“Desktop”选项卡，单击其中的 Web Browser，在打开的浏览器地址栏中输入http://192.168.0.1（访问 Wireless Router 的默认管理地址），按 Enter 键，如图 7-1-2 所示。

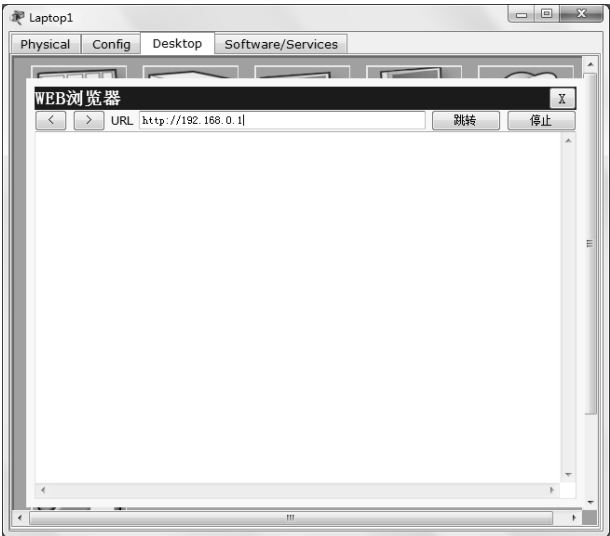


图 7-1-2 Web 浏览器

步骤 4：弹出如图 7-1-3 所示的“授权”对话框，提示输入用户名和密码。



图 7-1-3 “授权”对话框

步骤 5: 输入初始用户名 admin, 密码 admin, 单击“确定”按钮, 登录无线路由器 Wireless Router1, 进入 Web 管理界面, 如图 7-1-4 所示。



图 7-1-4 Web 管理界面

步骤 6: 无线路由器 Wireless Router1 的基本网络设置。

在如图 7-1-4 所示的界面中, 选择无线路由器 Web 管理界面中的“Setup 选项卡”, 输入无线路由器 Wireless Router0 的基本网络信息。这里将网络信息设置为静态 IP 模式, IP 地址为“172.16.0.100”, 子网掩码为“255.255.255.0”, 默认网关为“172.16.0.100”, 单击“保存配置”按钮后生效, 如图 7-1-5 所示。



图 7-1-5 配置静态 IP 地址



步骤 7：在该界面中还可以将无线路由器 Wireless Router0 的默认管理地址更改为 `http://192.168.0.1`，以及“启动”或“禁用”无线路由器 Wireless Router0 的 DHCP 服务（默认为启用状态），并配置 DHCP 服务的地址池，这里保持默认设置，如图 7-1-6 所示。



图 7-1-6 配置 DHCP 服务

步骤 8：在如图 7-1-4 所示的界面中，选择 Web 管理界面中的“Administration”选项卡，这里可以更改无线路由器 Wireless Router0 的登录密码，并设置是否允许远程管理等，如图 7-1-7 所示。



图 7-1-7 登录管理设置

步骤 9: 在如图 7-1-4 所示的界面中, 选择 Web 管理界面中的“Wireless”选项卡, 即可设置无线网络的基本参数, 如图 7-1-8 所示。这里将网络名称 SSID 设置为“caiwubu”即可(默认情况下, 该无线区域的登录密码为空)。



图 7-1-8 无线网络的基本参数设置

步骤 10: 登录并配置无线路由器 Wireless Router0。

在 Laptop1 上打开 Web 浏览器, 在浏览器的地址栏中输入 Wireless Router1 的默认管理地址“http://192.168.0.1”, 并按 Enter 键。将 Wireless Router1 设置为静态 IP 模式, IP 地址为 172.16.0.1, 子网掩码为 255.255.255.0, 默认网关为 172.16.0.1; 启用 DHCP 服务, 并配置 DHCP 服务的地址池, 即 192.168.0.100~192.168.0.120; 设置无线网络的网络名称 SSID 为“gongchengbu”(密码默认为空), 如图 7-1-9 所示。



图 7-1-9 无线网络 SSID 的设置

步骤 11: 配置移动终端 Tablet PC1, 将 Tablet PC1 加入 gongchengbu 无线网络。

单击 Tablet PC1, 在打开的窗口中选择“Config”→“Wireless0”选项, 在“SSID”文本框中填入“gongchengbu”即可, 如图 7-1-10 所示。

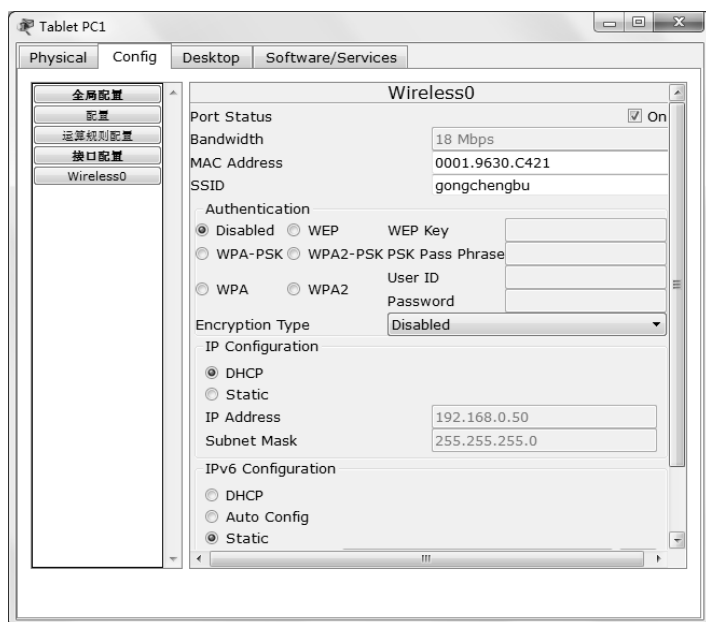


图 7-1-10 移动终端 Tablet PC1 的设置

步骤 12：配置移动终端 Tablet PC2，将该移动终端加入 caiwubu 无线网络即可。

单击 Tablet PC2，在打开的窗口中选择“Config”→“Wireless0”选项，在“SSID”文本框中填入“caiwubu”即可，如图 7-1-11 所示。

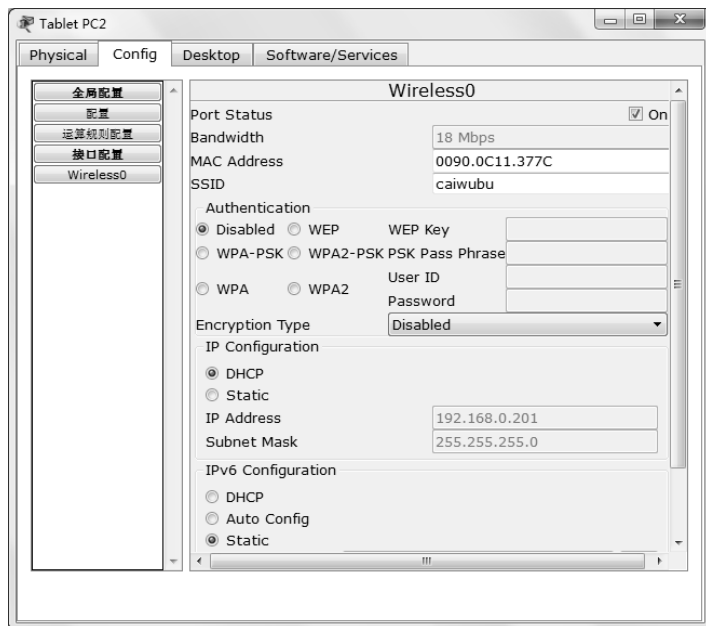


图 7-1-11 移动终端 Tablet PC2 的设置

步骤 13：测试两台无线终端到服务器的连通性。

(1) 移动终端 Tablet PC1 的测试如图 7-1-12 所示。

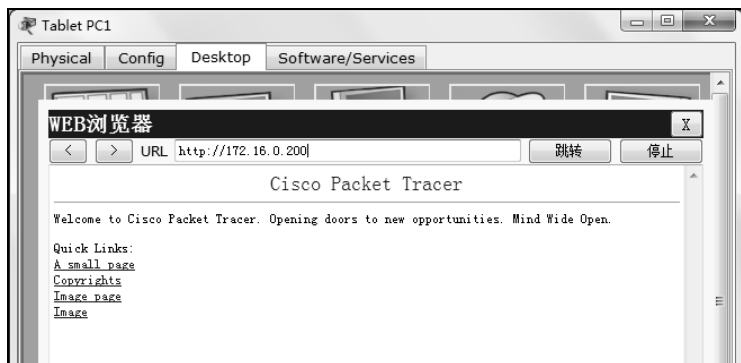


图 7-1-12 Tablet PC1 访问 Web 服务器

(2) 移动终端 Tablet PC2 的测试如图 7-1-13 所示。

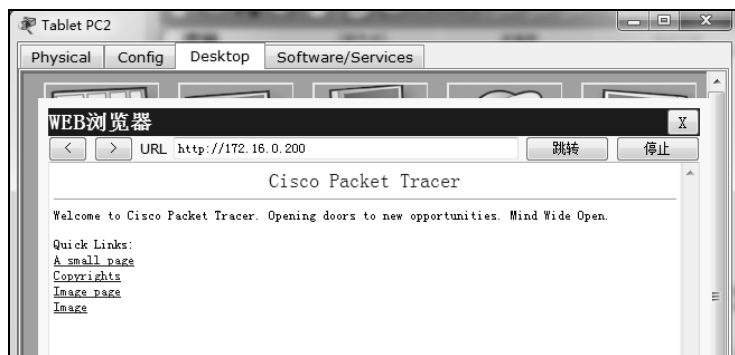


图 7-1-13 Tablet PC2 访问 Web 服务器

相关知识

WIFI (Wireless Fidelity) 是当今使用最广的一种无线网络传输技术, 实际上就是把有线网络信号转换为无线信号, 供支持其技术的相关计算机、手机、PDA 等接收。手机如果有 WIFI 功能, 在有无线信号的时候可以不通过数据网络上网, 省了流量费。而无线 AP 就是提供 WIFI 服务的重要设备。

网络模式: 802.11 无线 LAN 是一套 IEEE 标准, 该标准利用 2.4GHz 和 5GHz 频带的电磁波进行信号传输, 802.11 无线标准家族包括 802.11a/b/g/n 等多个标准。如果网络中有 Wireless-N、Wireless-G 和 Wireless-B 设备, 则可保持默认设置 Mixed。如果有 Wireless-G 和 Wireless-B 设备, 则可选择 BG-Mixed。如果只有 Wireless-N、Wireless-G 和 Wireless-B 中的一种设备, 则可选择对应的 Wireless-N Only、Wireless-G Only 和 Wireless-B Only。如果要禁用无线网络连接, 则可选择 Disable。

SSID 即服务集标识, 也称网络名称。SSID 技术可以将一个无线局域网分为几个需要不同身份验证的子网络, 每一个子网络都需要独立的身份验证, 只有通过身份验证的用户才可以进入相应的子网络, 防止未被授权的用户进入本网络。

频带: 要在使用 Wireless-N、Wireless-G 和 Wireless-B 设备的网络中获得最佳的性能, 则可保持默认设置自动。如果仅有 Wireless-N 设备, 则可选择 Wide-40MHz Channel。如果有 Wireless-G 和 Wireless-B 网络连接, 则应选择 Standard-40MHz Channel。



学习小结

本任务介绍了无线 AP 的功能和基本设置方法，读者应熟悉架设无线网络的基本步骤和流程，为下一步无线网络的安全管理打下基础。

实训 2 无线网络的安全管理

一旦某些入侵者通过无线网络连接到我们的 WLAN，那么他们就与那些直接连接到 LAN 交换机上的用户一样，对整个网络都有一定的访问权限。在这种情况下，除非事先已采取了一些措施，限制不明用户访问网络中的资源和共享文档，否则入侵者能够做授权用户所能做的任何事情。

学习情境

海成公司搭建了无线局域网，主要为了满足工程部和财务部移动办公的需要，但发现该无线网络存在一些安全问题，所有员工的手机和移动设备都可以自由接入本公司的无线网络，占用应用资源，影响了正常办公，需要对接入的设备数量和设备进行限定管理。

情境分析

海成公司的无线局域网确实存在安全隐患，现网络管理员准备设置工程部（gongchengbu）和财务部（caiwubu）都能够访问 Web 服务器，gongchengbu 无线网络配置接入密码为“nozu onodie”，caiwubu 无线网络配置接入密码为“LYP82NLF”；配置 caiwubu 的无线网络路由器，只允许无线终端 Tablet PC1 和 Tablet PC2 接入；配置 gongchengbu 无线网络路由器，只允许 3 台（含 3 台）以内的无线设备接入，以实现公司的无线网络的相对安全。

所需设备：

- (1) Cisco WRT300N 无线路由器 2 台。
- (2) Cisco Catalyst 2960 交换机 1 台。
- (3) Web 服务器 1 台。
- (4) 用户移动终端 6 台。
- (5) 直通线 4 条。
- (6) Console 线 1 条。

实训拓扑结构如图 7-2-1 所示。

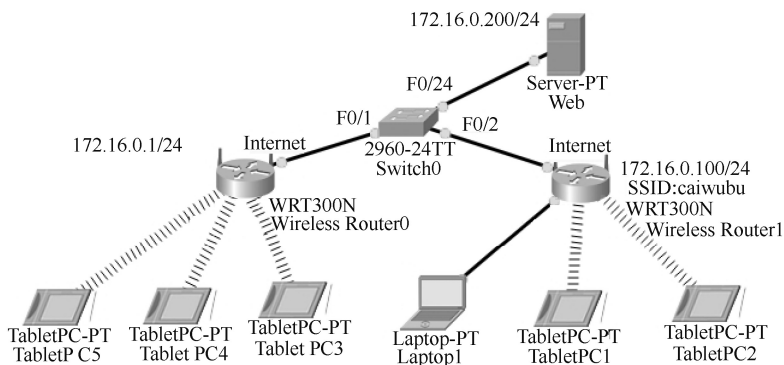


图 7-2-1 海成公司网络拓扑图

无线设备的 IP 地址和 SSID 分配情况如表 7-2-1 所示。

表 7-2-1 无线设备的 IP 地址和 SSID 分配情况

序号	名称	IP 地址	子网掩码	SSID
1	Wireless Router0	172.16.0.1	255.255.255.0	gongchengbu
2	Wireless Router1	172.16.0.100	255.255.255.0	caiwubu
3	Web 服务器	172.16.0.200	255.255.255.0	
4	Laptop1	自动获取		
5	Tablet PC3	自动获取		

步骤实现

步骤 1：按照图 7-2-1 连接网络拓扑结构。

步骤 2：按照表 7-2-1 配置笔记本式计算机和服务器的 IP 地址、子网掩码。

步骤 3：配置无线网络接入密码。登录无线网络路由器 Wireless Router0，进入无线路由器 Web 管理界面，选择“Wireless”→“Security”选项，在“安全模式”下拉列表中，将 Disabled 模式更换为其他安全模式，这里选择“WPA2 Personal”模式，如图 7-2-2 所示。

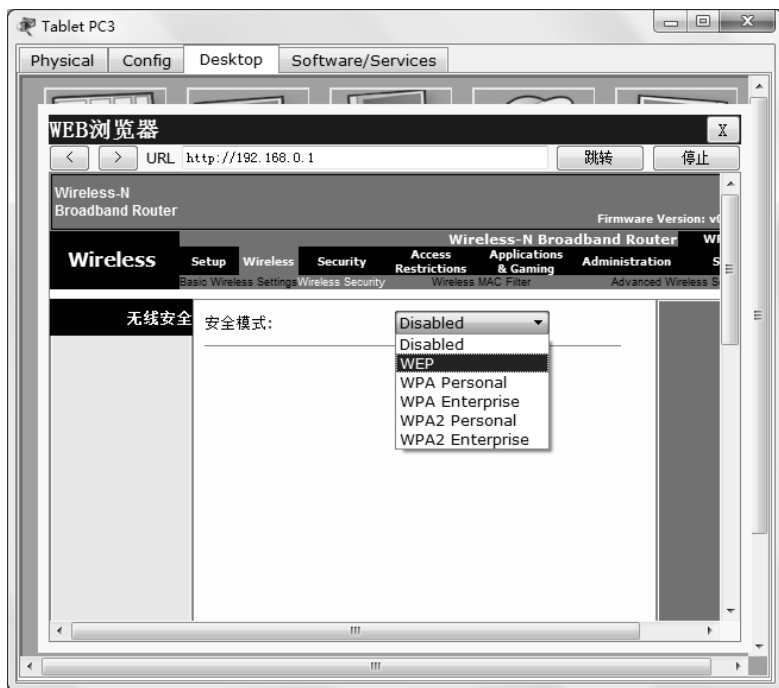


图 7-2-2 安全模式



小贴士

WEP: Wired Equivalent Privacy (有线等效保密) 的缩写，它是一种基本的加密方法，仍可支持较旧的设备，建议不要使用。启用 WEP 时，需设置网络安全密钥。该密钥可能会对一台计算机通过网络发送到另一台计算机的信息进行加密。但是，相对而言，WEP 安全机制比较容易破解。这里需要注意的是，因为 802.11n 不支持此加密方式，如果选择此加密方式，则路由器可能会工作在较低的传输速率上，Windows 7 也不支持使用 WEP 共享密钥身份验证自动设置网络。



WPA: WPA 的认证分为两种。第一种采用 802.1x+EAP 的方式, 用户提供认证所需的凭证, 如用户名和密码, 通过特定的用户认证服务器 (一般为 RADIUS 服务器) 来实现。在大型企业网络中, 通常采用这种方式, 即 WPA Enterprise。另外一种相对简单的模式, 它不需要专门的认证服务器, 这种模式被称为 WPA 预共享密钥 (WPA-PSK), 仅要求在每个 WLAN 结点 (AP、无线路由器、网卡等) 上预先输入一个密钥。只要密钥吻合, 客户即可获得 WLAN 的访问权, 即 WPA Personal。

WPA2: 顾名思义, 就是 WPA 的加强版, 也就是 IEEE 802.11i 的最终方案。它分为家用的 WPA2 Personal 与企业的 WPA2 Enterprise。WPA2 与 WPA 的差别在于, 它使用更安全的加密技术 AES, 因此比 WPA 更难被破解、更安全。因此, 如果可能, 应使用 WPA2。

步骤 4: 设置密码 “nozuonodie”, 保存配置即可, 如图 7-2-3 所示。



图 7-2-3 无线路由器设置安全密码

步骤 5: 配置完 Wireless Router0 登录密码后, 移动终端将自动离线。此时, 只要将移动终端加入 gongchengbu 无线网络即可。在 Cisco Packet Tracer 中, 单击 Tablet PC3, 在打开的配置中选择 “Config” 选项卡, 选择 “Wireless0” 选项, 在 “Authentication” 选项组中选中 “WPA2-PSK” 单选按钮, 在其密码栏内输入 “nozuonodie” 如图 7-2-4 所示, 将移动终端加入 gongchengbu 网络。



图 7-2-4 移动终端配置安全密码

步骤 6：将移动终端 Tablet PC3 重新加入 gongchengbu 无线网络，如图 7-2-5 所示。

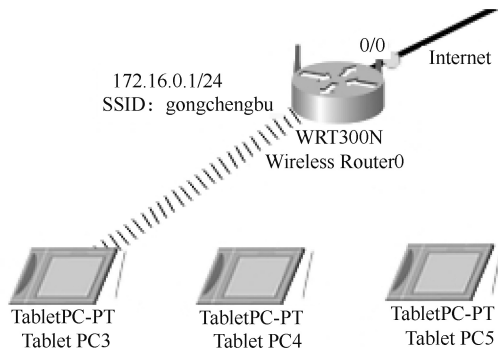


图 7-2-5 Tablet PC3 接入无线网络

步骤 7：以同样的方法，完成 Wireless Router1 的配置。

步骤 8：限定无线接入设备。

(1) 记录允许接入的移动终端的 MAC 地址，本例中为 0001.42B8.632B 和 0001.979B.1842，登录 caiwubu 无线网络路由器 Wireless Router1，选择无线路由器 Web 管理界面中的“Wireless”选项卡，再选择“Wireless MAC Filter”选项，如图 7-2-6 所示。

(2) 选择启用 Wireless MAC Filter，设置 Access Resolution 为“Permit PCs listed below to access wireless network”，即允许下列计算机接入无线网络。将相应的 MAC 地址按格式规范 00:01:42:B8:63:2B 和 00:01:97:9B:18:42 录入到 MAC 地址过滤列表中，保存配置即可。



图 7-2-6 Wireless MAC Filter 配置界面

步骤 8：测试。新加入一台移动设备，设置好加密方式和密码后，已经成功限制了 caiwubu 无线网络的接入。



步骤 9：限制无线接入设备的数量。采用限制 DHCP 中地址池对无线接入设备的数量进行简单限定。登录 gongchengbu 无线网络路由器 Wireless Router0，在 Setup 界面中，将“DHCP Server Settings”选项组中 DHCP 服务的“Maximum number”设置为“3”，如图 7-2-7 所示，保存配置后退出即可。



图 7-2-7 DHCP 地址池配置界面

相关知识

网络安全一直是一个永恒不变的话题。随着无线网络的流行，无线网络的安全问题更加突出。因为无线网络与有线网络相比，不需要物理上线路的连接，完全借助无线电磁波进行连接，因此更容易受到入侵。因为无线网的信号是在开放空间中传送的，所以只要有合适的无线客户端设备，在合适的信号覆盖范围之内就可以接收无线网卡的信号。无线网络存在的核心安全问题归结起来有如下 3 点。

1. 非法用户接入问题

Windows 操作系统基本上都具有自动查找无线网络的功能，只要对无线网络有基本认识，对于不设防或安全级别很低的无线网络，未授权的用户或黑客通过一般攻击或借助攻击工具都能够接入发现的无线网络。一旦接入，非法用户将占用合法用户的网络带宽，恶意的非法用户甚至能更改路由器的设置，导致合法用户无法正常登录，而有目的非法接入者还可能入侵合法用户的计算机窃取相关信息。

2. 非法接入点连接问题

无线局域网易于访问和配置简单的特性，使得任何人的计算机都可以通过自己购买的 AP，不经过授权而连入网络，有些企业员工为了方便使用，通常自行购买 AP，未经允许接入无线网络，这便是非法接入点，而在非法接入点信号覆盖范围内的任何人都可以连接和进入企业网络，这将带来很大的安全风险。

3. 数据安全问题

无线网的信号是在开放空间中传送的，通过获取无线网的信号，非法用户或恶意攻击者

有可能执行如下操作。

(1) 通过破解普通无线网络安全设置, 包括 SSID 隐藏、WEP 加密、WPA 加密、MAC 过滤等可以合法设备的身份进入无线网, 导致“设备身份”被冒用。

(2) 对传输信息进行窃听、截取和破坏。窃听以被动和无法觉察的方式入侵检测设备, 即使网络不对外广播网络信息, 只要能够发现任何明文信息, 攻击者仍然可以使用一些网络工具来监听和分析通信量, 从而识别出可以破坏的信息。

因此, 需要加强对无线网络的管理, 确保网络安全。

学习小结

本实训在熟悉无线网络的基本安全管理技术的基础上, 对无线网络的安全模式、接入密码设置、无线接入设备的 MAC 地址过滤和限制无线接入设备数量等进行了介绍。作为网络管理员, 需要增加对相关知识的了解, 以不断增强网络的安全性。

实训 3 有线和无线网络的全网互连

搭建有线、无线网络, 实现网络互连互通, 是网络管理员的基本任务。目前无线局域网还不能完全脱离有线网络, 无线网络与有线网络是互补的, 而不是竞争; 无线网络是有线网络的补充, 而不是替换。无线局域网以它的高速传输功能和灵活性发挥更加重要的作用。

学习情境

海成公司由于业务规模的扩大, 开设了分公司, 需要搭建分公司的网络, 该网络既有有线网络部分, 也有无线网络部分, 现需要实现内部网络的互连互通, 并且通过路由器共享获取 Internet 的访问资源。

情境分析

海成公司分公司的网络结合了有线、无线网络, 需要对整个网络进行设置, 为 Wireless Router 无线网络配置 SSID “wangluohutong”, 加密方式为 WAP2 Personal, 接入密码为 “wangluohutong”; 配置 Wireless Router 和 PC 1 在 VLAN 2, PC 2 在 VLAN 3; 配置路由器 GATE 的 G0/1 为内网接口, G0/0 为外网接口, 实现网络安全访问。

所需设备:

- (1) Cisco 2911 路由器 2 台。
- (2) Cisco WRT300N 无线路由器 1 台。
- (3) Cisco Catalyst 2960 交换机 1 台。
- (4) Web 服务器 1 台。
- (5) 用户终端 3 台。
- (6) 直通线 4 条。
- (7) 交叉线 2 条。
- (8) Console 线 1 条。

实训拓扑结构如图 7-3-1 所示。


```

Switch-A(vlan)#vlan 3 name vlan3
Switch-A(vlan)#exit
Switch-A#conf t
Switch-A(config)#int fa0/2
Switch-A(config-if)#switchport mode access
Switch-A(config-if)#switchport access vlan 2
Switch-A(config-if)#int range fa0/3-4
Switch-A(config-if-range)#switchport mode access
Switch-A(config-if-range)#switchport access vlan 3
Switch-A(config-if-range)#int fa0/1
Switch-A(config-if)#switchport mode trunk
Switch-A(config)#end
Switch-A#

```

步骤 4: 配置路由器 GATE 的主机名称, 配置 G0/1 端口的单臂路由, 实现 VLAN 和 VLAN 3 的通信。

```

Router>enable
Router#config terminal
Router(config)#host GATE
GATE(config)#int g0/1
GATE(config-if)#no ip add
GATE(config-if)#no shut
GATE(config-if)#int g0/1.2
GATE(config-subif)#encapsulation dot1Q 2
GATE(config-subif)#ip add 172.16.2.1 255.255.255.0
GATE(config-subif)#no shut
GATE(config-subif)#int g0/1.3
GATE(config-subif)#encapsulation dot1Q 3
GATE(config-subif)#ip add 172.16.3.1 255.255.255.0
GATE(config-subif)#no shut
GATE(config-subif)#end
GATE#

```

步骤 5: 配置路由器 GATE 的 G0/0 和 G0/1 端口的 IP 地址, 配置 GATE 的 ACL、NAT 和默认路由。

```

GATE#conf t
GATE(config)#access-list 1 permit 172.16.0.0 0.0.255.255
GATE(config)#ip nat inside source list 1 interface g0/0 overload
GATE(config)#interface g0/1
GATE(config-if)#no shutdown
GATE(config-if)#ip nat inside
GATE(config)#int g0/0
GATE(config-if)#no shutdown
GATE(config-if)#ip address 202.106.0.2 255.255.255.0

```




```
GATE(config-if)#ip nat outside
GATE(config-if)#exit
GATE(config)#ip route 0.0.0.0 0.0.0.0 202.106.0.1
GATE(config)#
```

步骤 6：配置路由器 ISP，配置路由器 Router1 两个端口的 IP 地址和默认路由。

```
Router>enable
Router#config terminal
Router(config)# hostname ISP
ISP(config)#int g0/0
ISP(config-if)#no shutdown
ISP(config-if)#ip address 202.106.0.1 255.255.255.0
ISP(config-if)#exit
ISP(config)#int g0/1
ISP(config-if)#no shutdown
ISP(config-if)#ip address 202.106.1.1 255.255.255.0
ISP(config-if)#exit
ISP(config)#ip route 0.0.0.0 0.0.0.0 202.106.0.2
ISP(config)#exit
```

步骤 7：配置无线路由器 Wireless Router 的 SSID 和相关 IP 地址。

配置无线路由器 Wireless Router 的 IP 地址为 172.16.3.10/24，配置无线网络 SSID 为“wangluohutong”，加密方式为 WAP2 Personal，接入密码为“wangluohutong”，设置 DHCP 服务。

登录无线网络路由器 Wireless Router，在 Setup 管理界面中，选择“Static IP”模式，输入 IP 地址“172.16.3.10”，子网掩码“255.255.255.0”，默认网关“172.16.3.1”，如图 7-3-2 所示，并保存配置。



图 7-3-2 设置无线路由器的参数

步骤 8：配置无线路由器 Wireless Router 的 SSID。

在 Web 管理界面中选择“Wireless”选项，将其网络名称 SSID 设置为“wangluohutong”，如图 7-3-3 所示。



图 7-3-3 设置无线路由器的 SSID

步骤 9: 配置无线路由器 Wireless Router 的无线接入密码。

选择图 7-3-3 所示的“Wireless Security”选项, 选择“WPA2 Personal”安全模式, 设置密码为“wangluohutong”, 如图 7-3-4 所示, 保存配置后退出即可。



图 7-3-4 设置无线路由器的登录密码

步骤 10: 设置移动用户终端 Tablet PC。

单击 PC2, 在打开的窗口中选择“Config”→“Wireless0”选项, 设置 Tablet PC 的 Wireless SSID 为“wangluohutong”, 密码为“wangluohutong”, 如图 7-3-5 所示即可。



图 7-3-5 Tablet 的 Wireless 设置



步骤 11：连接测试。

(1) 测试 PC1 能否访问 Web 服务器，如图 7-3-6 所示。

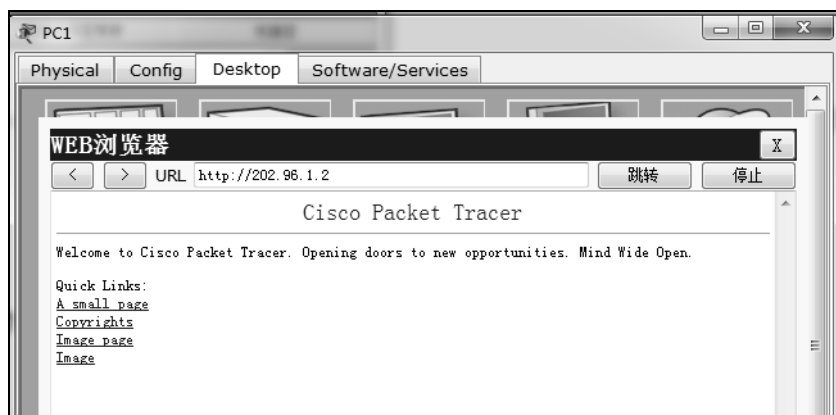


图 7-3-6 PC 1 访问 Web 服务器

(2) 测试 PC 2 能否访问 Web 服务器，如图 7-3-7 所示。

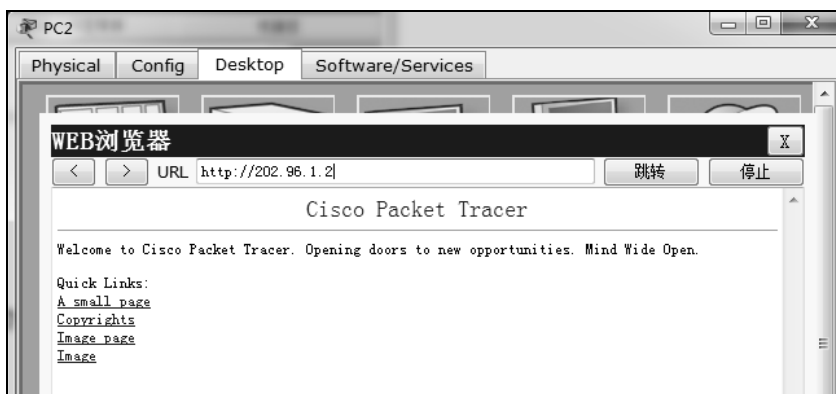


图 7-3-7 PC 2 访问 Web 服务器

(3) 测试 Tablet 能否访问 Web 服务器，如图 7-3-8 所示。

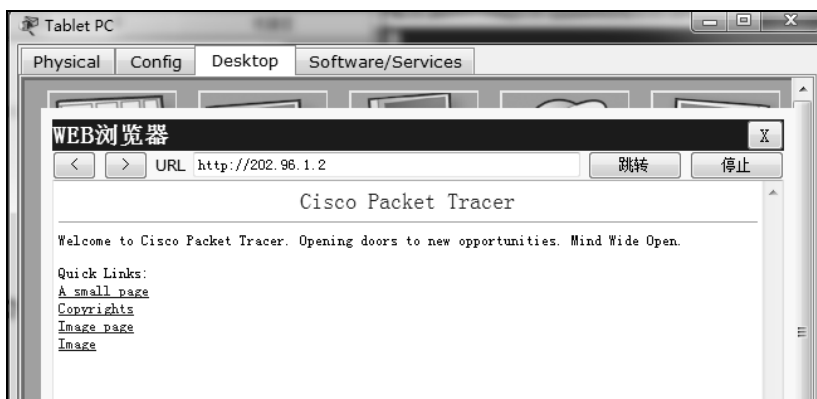


图 7-3-8 Tablet 访问 Web 服务器

学习小结

本实训介绍了有线网络和无线网络的综合，读者需要了解有线及无线网络的相关知识和技术，设置有线和无线的桥接，并配置无线 AP 的安全管理和控制，实现网络安全访问。

项目考核

海成公司搭建的无线网络 SSID 为 haicheng，采用 WPA2 Personal 加密方式，密钥为 1314iloveyou，如图 7-3-9 所示。

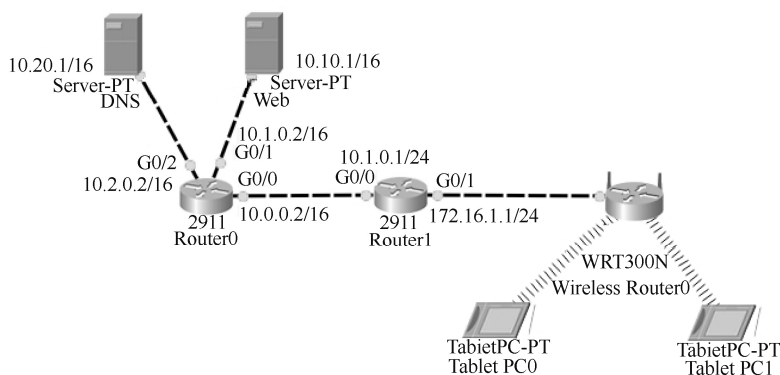
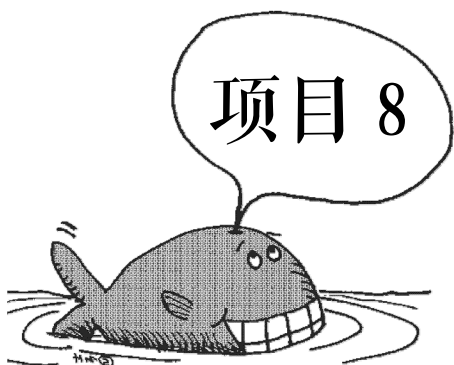


图 7-3-9 海成公司拓扑图

完成标准：无线网络实现 DHCP 服务。全网互连，PC0、PC1 可以自由访问 DNS 和 Web 服务器。



防火墙技术实现

项目学习说明

防火墙是一种用来加强网络之间访问控制的特殊网络互连设备，其核心是管理区域之间的访问控制。所以防火墙要将不同的接口置于不同的区域（不同区域的属性可以根据不同的接口命名来实现），然后对一个区域到另一个区域的访问进行安全控制。

尽管防火墙可能有其他附加功能，但本质还是管理区域之间访问的安全，在不安全的网络环境中构造一个相对安全的子网环境，按照事先制定的策略控制信息的流入和流出，监督和控制使用者的操作。

ASA 系列防火墙是 Cisco 2005 年推出的适应性安全产品，比 Cisco 原 PIX 系列专用的硬件防火墙功能强大，也更加人性化，更加容易配置和管理。Cisco ASA 防火墙 5500 系列自适应安全设备是最新的 Cisco 防火墙技术产品，它提供了整合防火墙、入侵保护系统（Intrusion Prevention System, IPS）、高级自适应威胁防御服务，包括应用安全和简化网络安全解决方案的 VPN 服务。

本项目以 Cisco-ASA-5505 防火墙为例，简单介绍防火墙的基本配置和防火墙的 DMZ 技术的实现。

学习能力目标

实训 1：防火墙的基本配置。

实训 2：防火墙 DMZ 技术。

职业能力目标

理解防火墙的基本原理、概念。

熟悉 Cisco-ASA 防火墙的作用和基本配置方法。

能够使用 Cisco-ASA 防火墙实现 DMZ 功能。

实训 1 防火墙的基本配置

从 Cisco Packet Tracer 6.1 开始, 支持防火墙 ASA 设备, 但支持 ASA 5505, 且功能有限, 如不支持 NAT 等高级配置。因此这里使用 Packet Tracer 做基本配置。

学习情境

海成公司由于业务规模的扩大, 购置了一台 Cisco 的防火墙, 型号为 ASA-5505, 要组建一个相对安全的网络系统, 确保公司员工的网络相对安全。

情境分析

规划与实施该项目时, 要先熟悉 Cisco-ASA-5505 的基本功能, 在掌握防火墙的技术特点的基础上, 启用相应的安全手段, 保障整个网络的正常运行。

要求 Inside 区域能够访问 Outside, 反之则受限, 防火墙对 DNS、FTP、HTTP、ICMP、TFTP、H323 等活动进行监控。

所需设备:

- (1) Cisco-ASA-5505 防火墙 1 台。
- (2) Cisco Catalyst 2960 交换机 1 台。
- (3) Cisco 2911 路由器 1 台。
- (4) Web 服务器 1 台。
- (5) PC 2 台。
- (6) 直通线 4 条。
- (7) Console 线 1 条。

实训拓扑结构如图 8-1-1 所示。

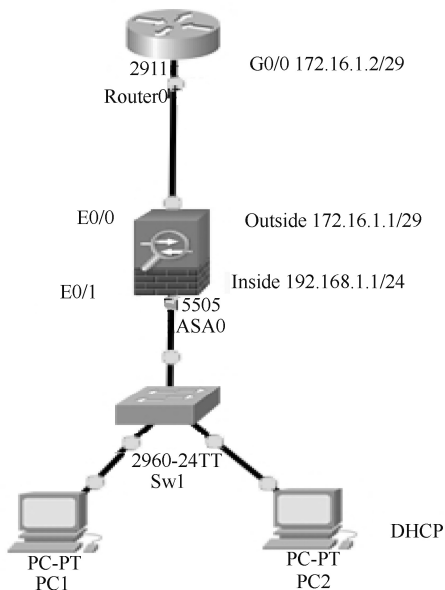


图 8-1-1 网络拓扑及结构



网络参数设置如表 8-1-1 所示。

表 8-1-1 网络参数设置

名称	端口	IP 地址	子网掩码
ASA0-5505	Outside (VLAN)	172.16.1.1	255.255.255.248
ASA0-5505	Inside (VLAN)	192.168.1.1	255.255.255.0
Cisco 2911	G0/0	172.16.1.2	255.255.255.248
PC 1	F0	自动获取	
PC 2	F0	自动获取	

步骤实现

步骤 1：按照图 8-1-1 连接网络拓扑。

步骤 2：配置防火墙的主机名称、VLAN 的 IP 地址和所属区域。

```
ciscoasa>en
Password:                ! 直接按 Enter 键即进入
ciscoasa#configure terminal
ciscoasa(config)#hostname FW
FW(config)#interface vlan 1      ! 进入 vlan1
FW(config-if)#nameif inside      ! 定义为内部区域
FW(config-if)#security-level 100 ! 安全级别为 100
FW(config-if)#ip address 192.168.1.1 255.255.255.0
FW(config-if)#no shutdown
FW(config-if)#exit
FW(config)#interface vlan2
FW(config-if)#nameif outside
FW(config-if)#security-level 0
FW(config-if)#ip address 172.16.1.1 255.255.255.248
FW(config-if)#no shutdown
FW(config-if)#exit
```



小贴士

Cisco-ASA-5505 是第二层的设备，不是第三层的，Cisco-ASA-5510 以上可以直接在接口上定义地址。5505 的地址配置在 VLAN 中，一般 Inside 为 VLAN 1，Outside 为 VLAN 2，把相应的端口划分到 VLAN 中，然后在 VLAN 上配置地址即可。

步骤 3：将端口 e0/0 加入到 VLAN 2，将 e0/1 加入到 VLAN 1 中。

```
FW(config)#interface e0/0
FW(config-if)#switchport access vlan 2
FW(config-if)#no shutdown
FW(config-if)#exit
FW(config)#interface e0/1
FW(config-if)#switchport access vlan 1
FW(config-if)#no shutdown
FW(config-if)#exit
```

步骤 4：配置路由和 NAT 转换。

```
FW(config)#route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
FW(config)#object network OBJ_GENERIC_ALL
```

```
FW(config-network-object)#subnet 0.0.0.0 0.0.0.0
```

```
FW(config-network-object)#nat (inside, outside) dynamic interface
```

步骤 5: 配置策略, 设置监测参数。

```
FW(config)#class-map inspection-default
```

```
FW(config-cmap)#match default-inspection-traffic
```

```
FW(config-cmap)#exit
```

```
FW(config)#policy-map type inspect dns preset-dns-map
```

```
FW(config-pmap)# parameters
```

```
FW(config-pmap-p)#message-length maximum 512
```

```
FW(config-pmap-p)#exit
```

```
FW(config-pmap)#exit
```

```
FW(config)#policy-map global-policy
```

```
FW(config-pmap)#class inspection-default
```

```
FW(config-pmap-c)#inspect dns preset-dns-map
```

```
FW(config-pmap-c)#inspect ftp
```

```
FW(config-pmap-c)#inspect http
```

```
FW(config-pmap-c)#inspect icmp
```

```
FW(config-pmap-c)#inspect tftp
```

```
FW(config-pmap-c)#inspect h323
```

```
FW(config-pmap-c)#exit
```

步骤 6: 应用路由策略, 配置 DHCP。

```
FW(config)#service-policy global-policy global ! 应用策略
```

```
FW(config)#dhcpd address 192.168.1.10-192.168.1.50 inside ! 配置 DHCP
```

```
FW(config)#dhcp enable inside ! 应用 DHCP
```

步骤 7: 测试。在 PC 1、PC 2 上 ping 路由器 G0/0, 以及在路由器 G0/0 上 ping PC1、PC2 有何区别?

在 PC1 上 ping 路由器 G0/0 端口时, 单击 PC 1, 在打开的窗口中选择“Desktop”选项卡单击“Command Prompt”图标, 在随后弹出的“命令提示符”对话框中, 键入 ping 172.16.1.2, 按 Enter 键进行测试, 结果如图 8-1-2 所示。

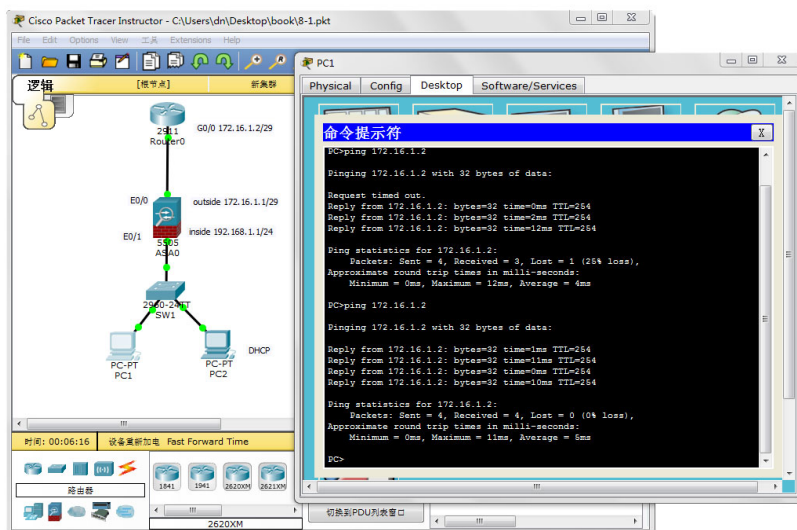


图 8-1-2 网络连通性测试



相关知识

ASA 是 Cisco 于 2005 年推出的防火墙和反恶意软件安全设备，现在的产品均是 5500 系列。企业版包括 4 种：Firewall、IPS、Anti-X 及 VPN。和 Cisco 以前的 PIX 系列防火墙类似，ASA 系列产品也提供了入侵防护系统及 VPN 集中器。图 8-1-3 所示为 Cisco ASA 5505 的外观图。



图 8-1-3 Cisco ASA 5505

1. 启用防火墙端口。

防火墙的端口要启用需要 3 个条件：一是设置 `nameif`；二是设置 `security-level`；三是设置 `ip addr`。防火墙默认的访问控制规则如下：从高安全级别端口发起的到低安全级别端口的访问都允许；从低安全级别端口发起的到高安全级别端口的访问都阻止；相同安全级别的端口不能互访，除非设置了 `same-security-traffic permit inter-interface`。

2. 安全级别

ASA 是一种基于状态的安全防护方式。每个进来的数据包（从低安全级别主机到高安全级别主机）都要根据 ASA 防火墙内存中的连接状态信息进行检查，并执行以下任务。

（1）对经过 ASA 防火墙的连接执行状态连接控制。

（2）对于内部应用，在没有明确配置的情况下，允许单向（出站）连接。出站的连接指从高安全级别接口向低安全级别接口的连接。

（3）监视返回的数据包，确认其有效性。

（4）对 TCP 序号进行随机处理，减少被攻击的可能性。

安全级别表明一个接口相对于另一个接口是可信的还是不可信的。如果一个接口的安全级别高于另一个接口的安全级别，则这个接口是可信的；如果一个接口的安全级别低于另一个接口的安全级别，则这个接口是不可信的。

安全级别的基本访问规则：具有较高安全级别的接口可以访问较低安全级别的接口。反之，较低安全级别的接口默认不能访问较高安全级别的接口，除非设置了 ACL 或。安全级别的范围是 0~100。下面分别介绍这些安全级别的规则。

（1）安全级别 100。这是 ASA 防火墙内部接口的最高级别，是默认设置，且不能改变。企业内部网络应该连接在该接口上。外部的网络不能访问该接口，而该接口可以任意访问其他接口。

（2）安全级别 0。这是 ASA 防火墙外部接口的最低级别，是默认设置，且不能改变。一般用以连接 Internet。

（3）安全级别 1~99。这是与 ASA 连接的边界接口的安全级别，可根据每台设备的访问情况来分配相应的安全级别。

（4）安全级别 100 访问安全级别 0 时，所有 IP 数据流都可以通行，除非设置了 ACL、

认证或授权的限制。虽然允许 IP 数据流通行，但仍然要通过 NAT 转换才能到达外网口。

(5) 安全级别 0 要访问安全级别 100 时，默认禁止所有 IP 数据流通行，除非设置了 ACL 允许数据流通过。认证和授权机制可进一步限制数据流的通行。

3. ASA 防火墙安全算法的原理

ASA 使用安全算法执行以下 3 项基本操作。

(1) 访问控制列表：基于特定的网络、主机和服务（TCP/UDP 端口号）控制网络访问。

(2) 连接表：维护每个连接的状态信息。安全算法使用此信息在已建立的连接中有效转发流量。

(3) 检测引擎：执行状态检测。检测规则集是预先定义的，用以验证应用是否遵从每个 RFC 和其他标准。

知识拓展

(1) `nameif` 命令用于定义端口类型。

`nameif` 命令的配置语法：

```
nameif name
```

`name` 通常设定为 `Inside`、`Outside` 和 `DMZ`，例如：

```
FW(config-if)#nameif outside
```

(2) `security-level` 命令用于配置接口的安全等级。

`security-level` 命令的配置语法：

```
security-level <0-100> Security level for the interface
```

`Inside` 默认安全级别为 100，`Outside` 默认安全级别为 0，`Inside` 安全级别 > `DMZ` 安全级别 > `Outside` 安全级别。

(3) `global` 用于指定公网地址范围，即定义地址池。

`global` 命令的配置语法：

```
global (if_name) nat_id ip_address-ip_address [netmark global_mask]
```

`(if_name)`：表示外网接口名称，一般为 `Outside`。

`nat_id`：建立的地址池标识(NAT 要引用)。

`ip_address-ip_address`：表示一段 IP 地址。

`[netmark global_mask]`：表示全局 IP 地址的网络掩码。

(4) NAT 地址转换命令用于将内网的私有 IP 转换为外网的公有 IP 地址。

NAT 命令的配置语法：

```
nat (if_name) nat_id local_ip [netmark]
```

`(if_name)`：表示接口名称，一般为 `Inside`。

`nat_id`：表示地址池，由 `global` 命令定义。

`local_ip`：表示内网的 IP 地址。0.0.0.0 表示内网所有主机。

`[netmark]`：表示内网 IP 地址的子网掩码。

(5) `route` 命令用于定义路由。

`route` 命令的配置语法：

```
route (if_name) 0 0 gateway_ip [metric]
```

`(if_name)`：表示接口名称。

0 0：表示所有主机。



gateway_ip: 表示网关路由器的 IP 地址或下一跳。

[metric]: 路由花费，默认值是 1。

(6) static 命令用于配置静态 IP 地址，使内部地址与外部地址一一对应。

static 命令的配置语法:

```
static(internal_if_name,external_if_name) outside_ip_addr inside_ip_address
```

internal_if_name: 表示内部网络接口，安全级别较高，如 Inside。

external_if_name: 表示外部网络接口，安全级别较低，如 Outside。

outside_ip_address: 表示外部网络的公有 IP 地址。

inside_ip_address: 表示内部网络的私有 IP 地址。

例如，asa(config)#static (inside, outside) 10.0.0.1 192.168.0.5，表示内部 IP 地址为 192.168.0.5，访问外部时被翻译为全局地址 10.0.0.1。

学习小结

本任务介绍了防火墙的基本概念，熟悉了 Cisco-ASA 系列防火墙关于安全级别的概念，读者要会定义 Cisco-ASA-5505 防火墙 Inside 及 Outside 接口和安全级别，并根据需要配置简单的路由及安全策略。

实训 2 防火墙 DMZ 技术

隔离区（Demilitarized Zone, DMZ）也称“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器，而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。通过 DMZ 区域，可以更加有效地保护内部网络，因为这种网络部署，比一般的防火墙更安全。

学习情境

海成公司购置了一台 Cisco-ASA-5505 防火墙，由于业务规模的扩大，访问 Web 服务器的人数越来越多，为了确保 Web 服务器的安全访问，可以将 Web 服务器等放置于 DMZ，用户在 Inside 可以正常访问网络。

情境分析

规划与实施该项目时，要熟悉 Cisco-ASA-5505 防火墙 DMZ 技术的特点，合理设置，保证整个网络的正常运行。

所需设备:

- (1) Cisco-ASA-5505 防火墙 1 台。
- (2) Cisco Catalyst 2960 交换机 2 台。
- (3) Cisco 2911 路由器 1 台。
- (4) DNS 服务器 1 台，Web 服务器 1 台。
- (5) PC 1 台。
- (6) 直通线 5 条。

(7) 交叉线 1 条。

(8) Console 线 1 条。

实训拓扑结构如图 8-2-1 所示。

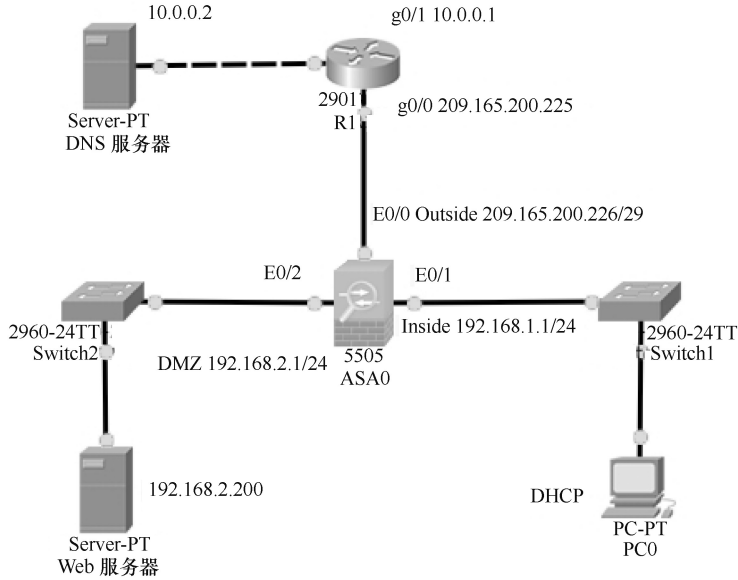


图 8-2-1 海成公司网络拓扑图

网络设备的端口及 VLAN 的 IP 地址分配如表 8-2-1 所示。

表 8-2-1 网络设备的端口及 VLAN 的 IP 地址分配

名称	端口	IP 地址	子网掩码	默认网关
ASA 5505	Inside (VLAN 1)	192.168.1.1	255.255.255.0	
	Outside (VLAN 2)	209.165.200.226	255.255.255.248	
	DMZ (VLAN 3)	192.168.2.1	255.255.255.0	
路由器 R1	G0/0	209.165.200.225	255.255.255.248	
	G0/1	10.0.0.1	255.255.255.248	
Web 服务器	F0	192.168.2.200	255.255.255.0	192.168.2.1
DNS 服务器	F0	10.0.0.2	255.255.255.248	10.0.0.1
PC0	F0	自动获取	自动获取	

步骤实现

步骤 1：按照图 8-2-1 连接网络拓扑。

步骤 2：按照表 8-2-1 配置服务器的 IP 地址、子网掩码和网关。

步骤 3：配置防火墙 VLAN 1、VLAN 2 和 VLAN 3 的 IP 地址，VLAN1 为 Inside，VLAN 2 为 Outside，VLAN 3 为 DMZ。

```
ciscoasa>enable
Password:
ciscoasa#configure terminal
ciscoasa(config)#host ASA5505
```



```
ASA5505(config)#interface vlan1
ASA5505(config-if)#nameif inside
ASA5505(config-if)#security-level 100
ASA5505(config-if)#ip address 192.168.1.1 255.255.255.0
ASA5505(config-if)#no shutdown
ASA5505(config-if)#exit
ASA5505(config)#interface vlan2
ASA5505(config-if)#nameif outside
ASA5505(config-if)#security-level 0
ASA5505(config-if)#ip address 209.165.200.226 255.255.255.248
ASA5505(config-if)#no shutdown
ASA5505(config-if)#exit
ASA5505(config)#interface vlan3
ASA5505(config-if)#nameif dmz
ASA5505(config-if)#security-level 50
ASA5505(config-if)#ip address 192.168.2.1 255.255.255.0
ASA5505(config-if)#no shutdown
ASA5505(config-if)#exit
```

步骤 4：在防火墙上，将端口 E0/0 加入 VLAN 2，E0/1 加入 VLAN 1，E0/2 加入 VLAN 3。

```
ASA5505(config)#interface e0/0
ASA5505(config-if)#switchport access vlan 2
ASA5505(config-if)#no shutdown
ASA5505(config-if)#exit
ASA5505(config)#interface e0/1
ASA5505(config-if)#switchport access vlan 1
ASA5505(config-if)#no shutdown
ASA5505(config-if)#exit
ASA5505(config)#interface e0/2
ASA5505(config-if)#switchport access vlan 3
ASA5505(config-if)#no shutdown
ASA5505(config-if)#exit
```

步骤 5：配置防火墙，定义相关参数，为地址区间命名。

```
ASA5505(config)#object-group service DM_INLINE_SERVICE_1
ASA5505(config-service-object-group)#service-object tcp destination eq 80
ASA5505(config-service-object-group)#service-object tcp destination eq 23
ASA5505(config-service-object-group)#service-object icmp
ASA5505(config-service-object-group)#exit
ASA5505(config)#object network Webserver
ASA5505(config-network-object)#host 192.168.2.200
ASA5505(config-network-object)#end
ASA5505#configure terminal
ASA5505(config)#object network Webserver-Ext
ASA5505(config-network-object)#host 209.165.200.230
```

```

ASA5505(config-network-object)#exit
ASA5505# configure terminal
ASA5505(config)#object network dmz-subnet
ASA5505(config-network-object)#subnet 192.168.2.0 255.255.255.0
ASA5505(config-network-object)#exit
ASA5505#configure terminal
ASA5505(config)#object network inside-subnet
ASA5505(config-network-object)#subnet 192.168.1.0 255.255.255.0
ASA5505(config-network-object)#exit

```

步骤 6: 配置防火墙, 设置访问控制列表, 应用到 Outside 端口的入站数据流上, 再配置 Outside 的默认路由。

```

ASA5505#configure terminal
ASA5505(config)#access-list Outside_access_in extended permit object-group
DM_INLINE_SERVICE_1 any object Webserver-Ext
ASA5505(config)#access-group Outside_access_in in interface outside
ASA5505(config)#route outside 0.0.0.0 0.0.0.0 209.165.200.225 1

```

步骤 7: 配置防火墙, 设置相关 NAT 转换。

```

ASA5505#configure terminal
ASA5505(config)#object network Webserver
ASA5505(config-network-object)#nat (dmz,outside) static 209.165.200.230
ASA5505(config-network-object)#exit
ASA5505(config)#object network dmz-subnet
ASA5505(config-network-object)#nat (dmz,outside) dynamic interface
ASA5505(config-network-object)#object network inside-subnet
ASA5505(config-network-object)#nat (inside,outside) dynamic interface

```

步骤 8: 配置防火墙, 设置策略参数。

```

ASA5505(config)#class-map global-class
ASA5505(config-cmap)#match default-inspection-traffic
ASA5505(config-cmap)#exit
ASA5505(config)#policy
ASA5505(config)#policy-map global-policy
ASA5505(config-pmap)#class global-class
ASA5505(config-pmap-c)#inspect dns
ASA5505(config-pmap-c)#inspect ftp
ASA5505(config-pmap-c)#inspect http
ASA5505(config-pmap-c)#inspect icmp
ASA5505(config-pmap-c)#inspect tftp
ASA5505(config-pmap-c)#inspect h323
ASA5505(config-pmap-c)#exit

```

步骤 9: 配置防火墙, 设置端口的 DHCP 服务。

```

ASA5505(config)#dhcp address 192.168.1.10-192.168.1.99 inside
ASA5505(config)#dhcpd dns 10.0.0.2 interface inside

```



```
ASA5505(config)#dhcpd enable inside
ASA5505(config)#dhcp address 192.168.2.10-192.168.2.99 dmz
ASA5505(config)#dhcpd dns 10.0.0.2 interface dmz
ASA5505(config)#dhcpd enable dmz
ASA5505(config)#dhcpd auto_config outside
```

步骤 10：配置路由器 R1 的主机名称及其接口 IP 地址。

```
Router>enable
Router#configure terminal
Router(config)#host R1
R1(config)#int g0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.248
R1(config-if)#no shut
R1(config)#int g0/1
R1(config-if)# ip address 10.0.0.1 255.255.255.248
R1(config-if)#no shut
R1(config)#ip route 0.0.0.0 0.0.0.0 G0/1
```

步骤 11：配置 DNS 服务器的 A 记录。单击 DNS 服务器，打开 DNS 配置窗口，在“Services”选项卡中选择 DNS 服务，设置 DNS 数据，添加“firewall.com”、www.firewall.com 的 A 记录，如图 8-2-2 所示。

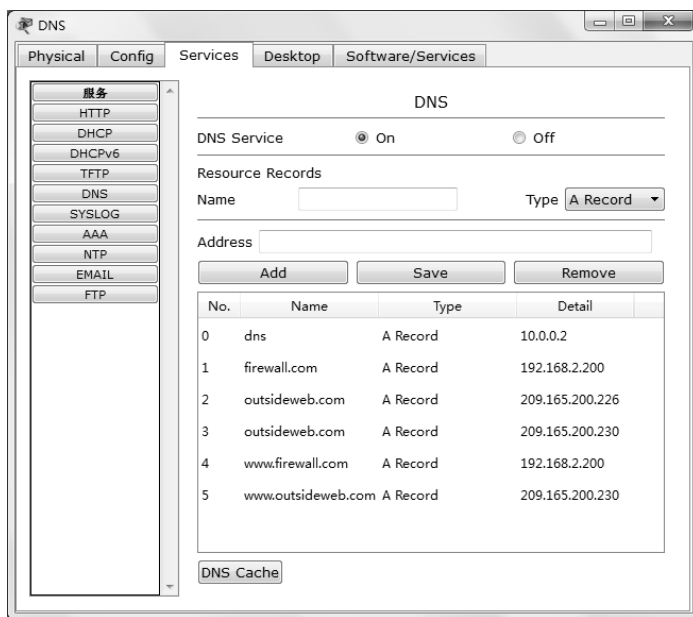


图 8-2-2 DNS 服务器 A 记录设置

步骤 12：配置 Web 服务器。单击 Web 服务器，打开 Web 配置窗口，在“Services”选项卡中选择 HTTP 服务，编辑网页信息，如图 8-2-3 所示。

步骤 13：测试连通性。

(1) 单击计算机 PC0，在打开的窗口中选择“Desktop”选项卡，单击“Web Browser”图标，如图 8-2-4 所示。

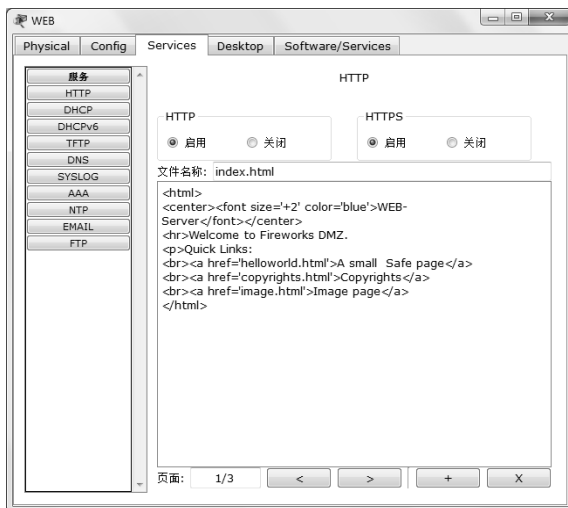


图 8-2-3 Web 服务器网页设置



图 8-2-4 “Desktop”选项卡

(2) 在打开的 Web 浏览器的地址栏中输入“http://www.firewall.com”，测试结果如图 8-2-5 所示。

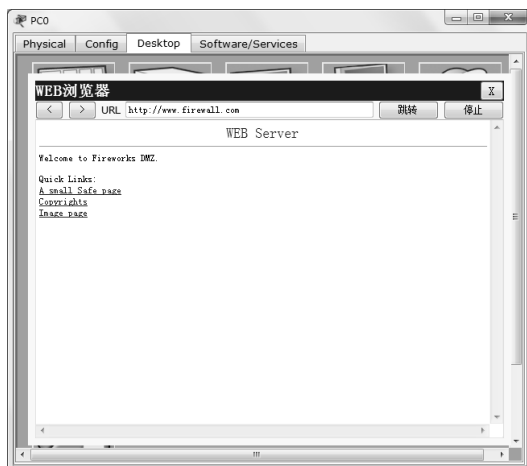


图 8-2-5 测试结果页面



相关知识

将部分用于提供对外服务的服务器主机划分到一个特定的子网——DMZ 中，DMZ 中的主机能与同处 DMZ 内的主机和外部网络的主机通信，而同内部网络主机的通信会受到限制。这使 DMZ 的主机能被内部网络和外部网络访问，而内部网络又能避免外部网络的侵入。

因此将网络划分为 3 个区域：安全级别最高的 LAN Area（Inside），安全级别中等的 DMZ 和安全级别最低的 Internet 区域（Outside）。3 个区域因担负不同的任务而拥有不同的访问策略。防火墙 DMZ 的网络结构如图 8-2-6 所示。

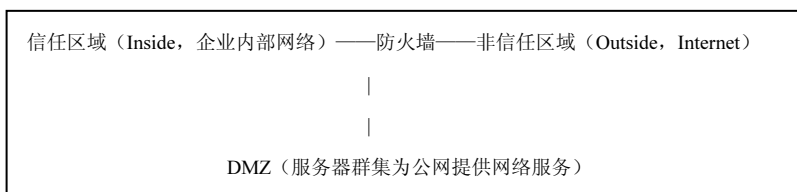


图 8-2-6 防火墙 DMZ 网络结构

其访问权的权限如下：信任区域可以任意访问所有区域；DMZ 不能主动访问信任区域，但是可以访问非信任区域；非信任区域不能主动访问信任区域，但是可以访问 DMZ。

学习小结

本实训介绍了防火墙的 DMZ 的基本概念和相关设置，要求读者熟悉 Cisco-ASA 关于访问控制列表、NAT 转换和策略参数及其设置的一般方法，并能够灵活使用。

项目考核

某公司使用防火墙将内部网络划分为 Inside、Outside、DMZ 3 个区域，DMZ 为安全服务器区，Outside 为外部自由工作区，Inside 为内部工作区。要求内部工作区的用户能够自由访问 DMZ 和 Outside 的服务器，而 Outside 用户只能有限地访问 DMZ 的 Web1 服务器。网络拓扑如图 8-2-7 所示，要求实现防火墙 ASA-5505 的配置。

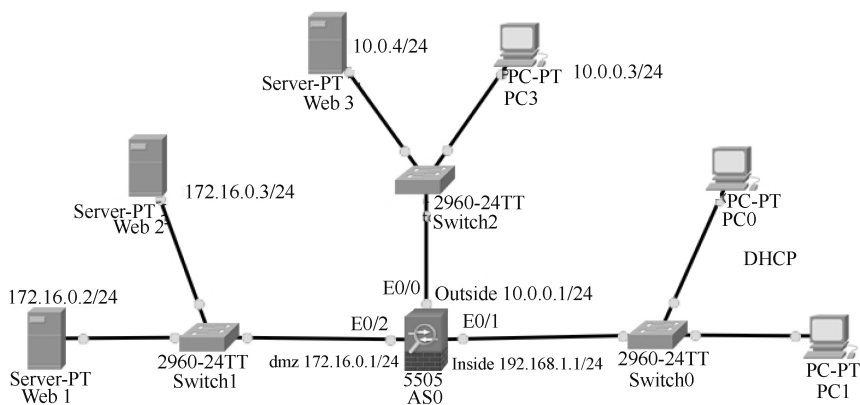
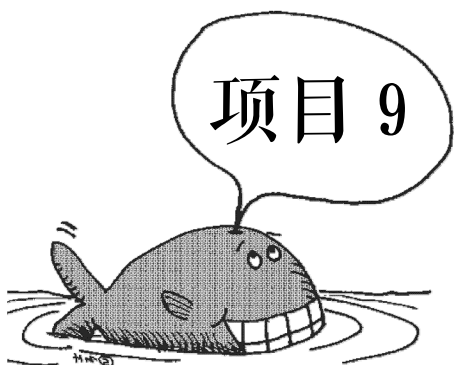


图 8-2-7 某公司内部网络拓扑图



综合实训

项目学习说明

本项目重点针对网络设备的综合应用进行讲述，为学习网络课程的初学者设计、配置、排除网络故障提供了良好的案例，使初学者更熟悉网络设备的配置和在实际企业中的综合应用。

在本项目中，根据实际工作的要求，专门设计下两个实训来学习网络的综合应用。

学习能力目标

实训 1：小型企业的网络工程案例。

实训 2：企业网络综合实训。

职业能力目标

能完成小型企业网络设备的配置。

能综合运用网络设备的相关技术实现企业的需求。

实训 1 小型企业的网络工程案例

本实训不仅将前几个项目所学的基本知识进行了巩固，使读者熟练掌握前面项目所学的知识，还能学习到一些网络设备配置方面更高层次的应用，了解 VPN 等的应用。

学习情境

海成公司总部设在广州，由于业务发展的需要，准备在深圳开设分公司，为了实现快捷的信息交流和资源共享，需要构建一个跨地域的企业网络。总公司设有销售部和管理部两个



部门，分公司设有销售部。

总公司采用双核心交换机的网络架构，独立设置公共服务网络部分，确保内部网络安全。

为了实现快捷的信息传递和满足公司业务的需求，允许分公司办公的员工能够方便、快捷、安全地访问总公司的内网服务器群。

外网采用 OSPF 动态路由协议，总公司内部和分公司内部采用私有地址和 RIPv2，内部访问外部采用 NAT。

情境分析

1. 网络连接

根据需求分析与下列详细要求完成网络结构的设计与设备的连接，画出完整的网络拓扑结构图。拓扑结构图中需要明确列出设备接线的端口号，以及相关端口的 IP 地址。实际接线与设置必须按照拓扑结构图进行。

完成网络的规划设计后，按以下要求进行网络的连接与配置。

(1) 总公司使用一台路由器的网络出口接入互联网，总公司内部访问外部采用 NAT，PC7 模拟互联网上的计算机。

(2) 总公司的路由器分别下连两台三层交换机作为汇聚交换机，分别通过三层互连；两台三层汇聚交换机之间通过两条线路进行链路汇聚通信，留出一条线路作为链路备份，两台汇聚交换机下连两台接入交换机，并形成冗余链路，实现对客户的透明传输。

(3) 总公司内部的路由器和汇聚交换机之间使用 RIPv2 路由协议，实现内部网络的互相通信。

(4) Switch-C 位于 9 楼办公室，Switch-D 位于 10 楼办公室，分别接有不同部门的员工机器。

(5) PC 1 和 PC 2 接入二层交换机 Switch-C，PC3 和 PC4 接入二层交换机 Switch-D；PC1 和 PC3 属于一个部门，划归 VLAN 10；PC 2 和 PC 4 属于一个部门，划归 VLAN 20。

(6) PC 1~PC 4 通过汇聚交换机 Switch-B 自动获取 IP 地址。

(7) 分公司与公网之间使用 PPP 进行连接。

(8) 分公司使用一台路由器的网络出口接入互联网，分公司使用一台路由器与运营商路由器通过 VPN (IPSec) 技术互连。

(9) 分公司的路由器下连一台二层交换机作为接入交换机，接入交换机下连两个部门的员工机器。

(10) PC 5 和 PC 6 接入二层交换机 Switch-E；PC 5 属于一个部门，划归 VLAN 70；PC 6 属于一个部门，划归 VLAN 80。

(11) PC5 和 PC6 通过公网的 Router-B 获取 IP 地址，且 PC 5 和 PC 6 可以相互通信。

(10) 总公司、分公司与公网的外网之间使用 OSPF 路由协议，实现内部和外部网络的互相通信。

(13) 根据设计估算所需要的耗材数量，准备好材料清单。

(14) 根据上述要求完成拓扑设计后，制作线缆，完成设备的连接。

(15) 打配的跳线使用 T568B 线序，制作的线缆必须稳固、耐用。

根据设计要求，拓扑结构如图 9-1-1 所示，按图 9-1-1 中的要求完成相关网络设备的连接。

所需设备。

- (1) Cisco WS-C3560 交换机 2 台。
- (2) Cisco WS-C2960 交换机 3 台。
- (3) Cisco 2911 路由器 3 台。
- (4) 模拟服务器的计算机 2 台。
- (5) PC 7 台。
- (6) 直连和交叉双绞线若干条。
- (7) Console 线 1 条。
- (8) V.35 DTE-V.35 DCE 线缆 2 条。

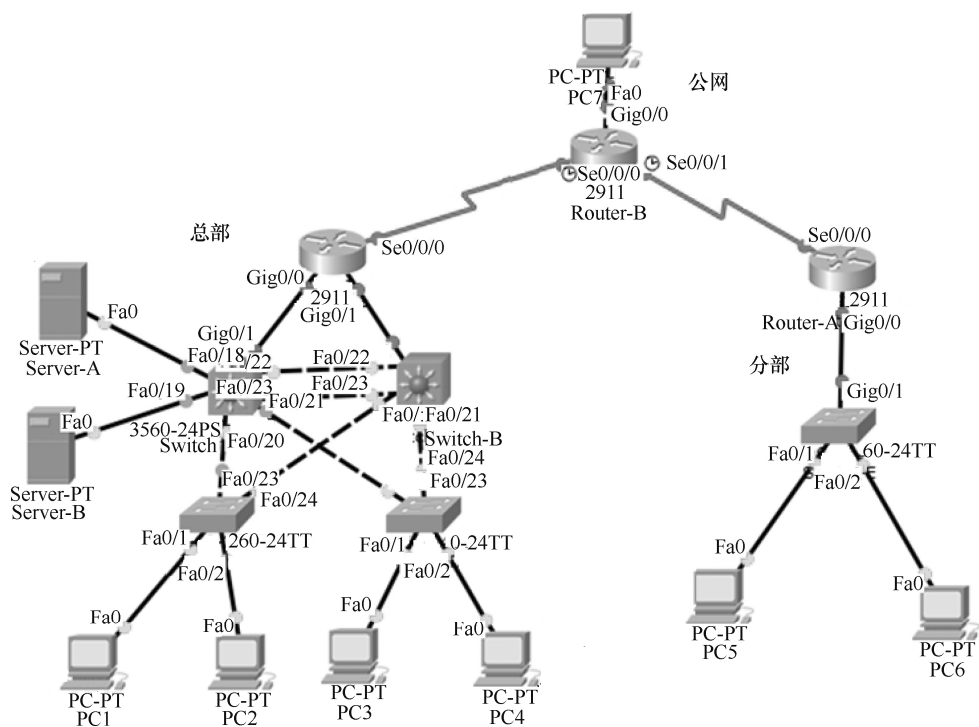


图 9-1-1 网络互联的拓扑结构

2. 地址规划

根据要求确定各接口的 IP 地址，如表 9-1-1 所示。

表 9-1-1 IP 地址的配置

设备名称	设备型号	设备接口	IP地址
Router-A	Cisco 2911	S0/0/0	140.10.1.5/30
		G0/0	192.168.10.37/30
		G0/1	192.168.10.41/30
Router-B	Cisco 2911	S0/0/0	140.10.1.6/30
		S0/0/1	150.10.1.5/30
		G0/0	160.10.1.5/24



（续）

设备名称	设备型号	设备接口	IP地址
Router-C	Cisco 2911	S0/0/0	150.10.1.6/30
		G0/0.1	172.16.70.254/24
		G0/0.2	172.16.80.254/24
Switch-A	Cisco WS-C3560	G0/1	192.168.10.38/30
		VLAN 100 SVI（服务器群）	192.168.10.65/27
		VLAN 10 SVI（销售部）	192.168.10.97/27
		VLAN 20 SVI（管理部）	192.168.10.129/27
		Port-channel 1（Port 22 和 23）	192.168.10.45/30
Switch-B	Cisco WS-C3560	G0/1	192.168.10.42/30
		VLAN 10 SVI（销售部）	192.168.10.126/27
		VLAN 20 SVI（管理部）	192.168.10.158/27
		Port-channel 1（Port22 和 23）	192.168.10.46/30
Switch-C	Cisco WS-C2960	与 sw1 和 sw2 采用标准协议连接	划分 VLAN 10 和 VLAN 20
Switch-D	Cisco WS-C2960	与 sw1 和 sw2 采用标准协议连接	划分 VLAN 10 和 VLAN 20
Switch-E	Cisco WS-C2960	与 Router-C 采用标准协议连接	划分 VLAN 70 和 VLAN 80
Server-A		属于 VLAN 100	192.168.10.66/27
Server-B		属于 VLAN 100	192.168.10.67/27
PC 1		属于 VLAN 10	DHCP（Switch-B）获得 IP 网段
PC 2		属于 VLAN 20	
PC 3		属于 VLAN 10	
PC 4		属于 VLAN 20	
PC 5		属于 VLAN 70	DHCP（Router-B）获得 IP 网段
PC 6		属于 VLAN 80	
PC 7		与 Router-B 的以太网口相连	160.10.1.6/24

3. 任务要求

（1）根据给出的拓扑结构图配置设备名称。

（2）在所有网络设备上为特权用户增加密码：passwordden，密码以加密方式存储。

（3）在各三层交换机和路由器上设置 Telnet 登录，登录用户名为 usertest，密码为 passwordtest，密码以明文方式存储，路由器中的登录验证方法名为系统默认名称，此方法使用本地数据库验证；在路由器 Router-C 上为特权用户添加密码 passenable，用户级别为最高级，密码以明文方式存储。

（4）在三层交换机 Switch-A 上划分各 VLAN，并加入相应的端口，如表 9-1-2 所示。

表 9-1-2 Switch-A 的 VLAN 划分

VLAN	名称	端口号
VLAN 100	Dept01	
VLAN 20	Dept02	
VLAN 100	Server	E0/0/18、E0/0/19

表 9-1-2 中未提到的端口，均划分到 VLAN 1 中。

（5）在三层交换机 Switch-B 上划分各 VLAN，并加入相应的端口，如表 9-1-3 所示。

表 9-1-3 Switch-B 的 VLAN 划分

VLAN	名称	端 口 号
VLAN 10	Dept01	
VLAN 20	Dept02	

表 9-1-3 中未提到的端口，均划分到 VLAN 1 中。

(6) 在二层交换机 Switch-C 上划分各 VLAN，并加入相应的端口，如表 8-1-4 所示。

表 9-1-4 Switch-C 的 VLAN 划分

VLAN	名称	端 口 号
VLAN 10	Dept01	E0/0/1、E0/0/11-E0/0/13
VLAN 20	Dept02	E0/0/2、E0/0/14-E0/0/16

表 9-1-4 中未提到的端口，均划分到 VLAN 1 中。

(7) 在二层交换机 Switch-D 上划分各 VLAN，并加入相应的端口，如表 9-1-5 所示。

表 9-1-5 Switch-D 的 VLAN 划分

VLAN	名称	端 口 号
VLAN 10	Dept01	E0/0/1、E0/0/11-E0/0/13
VLAN 20	Dept02	E0/0/2、E0/0/14-E0/0/16

表 9-1-5 中未提到的端口，均划分到 VLAN 1 中。

(8) 根据拓扑结构图在各交换机上创建各 VLAN，给虚拟接口配置 IP 地址（VLAN 1 为管理 VLAN）。

(9) 在汇聚层和接入层的交换机上配置路由冗余协议和多生成树协议，使总公司员工能够安全稳定地使用网络工作。

(10) 在 Switch-B 上实现 DHCP 服务器，要求为 PC1、PC2、PC3 和 PC4 所在的子网提供自动分配 IP 地址的服务，租期为 4 天。

(11) 为 Switch-A 的端口 4 设定端口带宽限制，出入口均限速 1Mb/s。

(12) 为 Switch-B 的端口 8 上配置广播风暴抑制，允许通过的广播包为 5000/s。

(13) 根据拓扑结构图，将 3 台路由器的 serial 口用背对背线缆连接，带宽为 2048000b/s，线缆连接时，要注意确保 Router-C 为 DTE 端，Router-B 为 DCE 端，速率为 2048000b/s。封装需要进行 CHAP 验证的 PPP，验证方法列表名为 test；DCE 端的路由器用户名为 userdce，密码为 chappass；DTE 端的路由器用户名为 userdte，密码为 chappass，密码用明文显示。

(14) 根据拓扑结构图在各路由器的相关位置配置 IP 地址，对快速以太网口添加描述，明确连接对象。

(15) 总公司内部配置动态路由协议 RIPv2，分公司内部配置动态路由协议 RIPv2，使全网连通，总公司、分公司与公网的外网之间使用 OSPF 路由协议，实现内部和外部网络的通信。

(16) 在 Router-B 上实现 DHCP 服务器，要求为 PC5 和 PC6 所在的子网提供自动分配 IP 地址服务。

(17) 在 Router-B 上实现单臂路由，使 PC5 和 PC6 可以相互通信。

(18) 路由器快速以太网口速率为 100Mb/s 在全双工模式。

(19) 上班时间禁止 PC1 所在网段访问 PC7 所在网段，ACL 名称为 worktime。



(20) Switch-D 上实现 PC4 的 MAC 地址与 E0/0/2 端口的绑定, 该端口的最大安全 MAC 地址数为 3, 锁定该端口。

(21) 配置 Switch-B, 使其能够通过 Web 方式访问交换机, Web 授权用户为 admin, 口令为加密的 adminpass。

(22) 禁止 PC 2 ping PC 6, 但 PC 6 可以连通 PC 2。

(23) 完成配置后将各设备的配置文件捕获为 TXT 格式, 并保存此文字。

步骤实现

详细配置参见教学指导素材。

学习小结

本实训综合应用到了本书所学的二层交换机、三层交换机和路由器配置的基本知识, 主要包括交换机配置文件清空、交换机配置模式、交换机命名、基于端口的 VLAN 划分、VLAN 接口的 IP 地址配置、特权密码、Telnet 登录交换机、链路聚合、生成树协议、虚拟网关路由协议、三层路由通信和路由器的命名、单臂路由、RIP、OSPF、广播风暴、PPP、VPN、DHCP、ACL 和 NAT 等知识。

实训 2 企业网络综合实训

学习情境

海成公司由于公司业务规模的扩大, 现分为东区和西区, 两个厂区相隔不远。东西两厂区之间准备通过路由器的 VPN 技术实现互连。东厂区作为公司互联网的出口, 东西两个厂区均通过该接口访问互联网。公司的主要服务器放在东厂区防火墙的 DMZ 中。在西厂区中使用两台三层交换机作为双核心交换机, 交换机设置链路聚合以提高交换机之间的带宽。另外, 交换机之间还提供了一条线路作为备份链路, 以备聚合链路出现故障时使用。西厂区各大楼划分 VLAN 管理。两厂区之间的数据通过 VPN 实现加密传输。要求优化网络配置, 使整个公司网络高效、稳定、安全。公司需要搭建多种网络服务, 提供主页发布、文件共享、邮件收发等常用功能。公司为方便会议使用网络和来访客户使用互联网, 特意架设了无线网络。

情境分析

1. 网络连接

根据需求分析与下列详细要求完成网络结构的设计与设备的连接, 画出完整的网络拓扑结构图。拓扑结构图中需要明确列出设备接线的端口号, 以及端口相关的 IP 地址。实际接线与设置必须按照拓扑结构图进行。

完成网络的规划设计后, 按以下要求进行网络的连接与配置。

(1) 东厂区使用一台防火墙作为网络唯一出口并接入互联网, PC 1 模拟互联网上的计算机; Server 接入该防火墙的 Eth0/4, 作为公司网内服务器。

(2) 西厂区使用一台路由器与东厂区路由器通过 VPN 技术互连; 东厂区的路由器通过 F0/0 口与防火墙相连; 西厂区的路由器分别下连两台三层交换机作为汇聚交换机, 通过三层互连; 两台三层汇聚交换机之间通过两条线路进行链路汇聚通信, 留出一条线路作为链路备份, 汇聚交换机下连一个接入层交换机。

- (3) 无线 AP 接在汇聚交换机上, 通过 AP 可以实现无线上网。
- (4) PC1 和 PC2 接入二层交换机, PC1 和 PC2 的 IP 地址自动获取, 服务器为 Switch-A。PC1 划归 VLAN 10, PC2 划归 VLAN 20。
- (5) 根据设计估算所需要的耗材数量, 准备好材料清单。
- (6) 根据上述要求完成拓扑设计后, 制作线缆, 完成设备的连接。
- (7) 打配的跳线使用 T568B 线序, 制作的线缆必须稳固、耐用。
- 根据要求画出公司的网络拓扑图, 如图 9-2-1 所示。

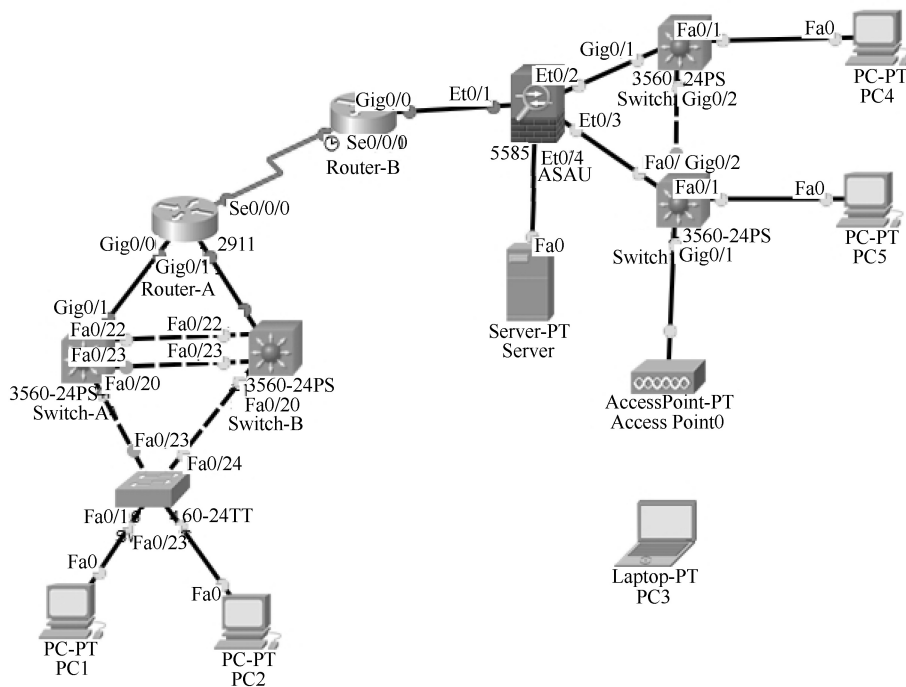


图 9-2-1 公司网络拓扑



小贴士

- (1) 画图时应标出各设备名、所连端口号。
- (2) PC 和路由器相连、交换机和交换机相连时必须使用交叉线。
- (3) 线路连接好后应检查指示灯是否工作正常。

所需设备:

- (1) DCRS-5650 交换机 2 台。
- (2) DCS-3950 交换机 1 台。
- (3) DCR-2626 路由器 2 台。
- (4) DCFW-1800 防火墙 1 台。
- (5) DCWL-7962AP 1 台。
- (6) PC 4 台。
- (7) 带无线网卡的笔记本式计算机 1 台。
- (8) Console 线 1 条。
- (9) V.35 DTE-V.35 DCE 线缆 2 条



2. 网络地址划分

(1) Router-A 的 S0/0/0 端口 IP 地址为 172.16.1.1/30，Router-B 的 S0/0/0 端口 IP 地址为 172.16.1.2/30，作为厂区间互连地址。

(2) 东厂区使用 172.16.2.0/24 作为内部网络地址段，以最后一个有效 IP 地址作为网关，Server 主机使用第一个有效 IP 地址作为地址。

(3) 东厂区路由器的防火墙接入互联网地址为 10.10.10.1/30。PC 4 和 PC 5 是东厂区内网中的机器。

(4) 东厂区路由器 G0/0 端口 IP 地址为 172.16.1.5/30；东厂区防火墙 E0/1 端口 IP 地址为 172.16.1.6/30。

(5) 西厂区有 2 栋办公楼，每栋办公楼有 40~50 个用户。使用 192.168.1.0/24 网段进行子网规划，划分 2 个 VLAN，分别为 VLAN 10 和 VLAN 20。VLAN 10 使用 192.168.1.0/24 网段子网划分后的第一个有效子网。VLAN 20 使用 192.168.1.0/24 网段子网划分后的第二个有效子网。使得每栋楼都有一个独立的网段，每个网段的网关使用该网段最后一个有效网络地址。

(6) 二层交换机 Switch-A 的 1、3~10 号端口划归 VLAN 10，2、11~19 号端口划归 VLAN 20，根据子网规划，在网络设备中设定 VLAN。

(7) 交换机的端口地址（各子网网关的端口地址根据要求设定）：

Switch-A 端口 24 指定网关路由地址为 192.168.2.1/24。

Switch-B 端口 24 指定网关路由地址为 192.168.3.1/24。

(8) Router-A 以太网端口地址：G0/0 IP 地址为 192.168.2.2/24，G0/1 IP 地址为 192.168.3.2/24。

根据要求确定各接口 IP 地址，如表 9-2-1 所示。

表 9-2-1 各接口的 IP 地址

设 备	端 口	IP 地址	网 关
Router-A	S0/0/0	172.16.1.1/30	无
Router-A	G0/0	192.168.2.2/24	无
Router-A	G0/1	192.168.3.2/24	无
Router-B	G0/0	172.16.1.5/30	无
Router-B	S0/0/0	172.16.1.2/30	无
Switch-A	G0/1	192.168.2.1/24	无
Switch-A	VLAN 10	192.168.1.125/26	无
Switch-A	VLAN 20	192.168.1.189/26	无
Switch-B	G0/1	192.168.3.1/24	无
Switch-B	VLAN 10	192.168.1.126/26	无
Switch-B	VLAN 20	192.168.1.190/26	无
Switch-C	VLAN 10	无	无
Switch-C	VLAN 20	无	无
Switch-D	F0/24	10.10.10.2/30	
Switch-D	VLAN 10	10.10.10.9/30	
Switch-E	F0/24	10.10.10.6/30	
Switch-E	VLAN 20	10.10.10.13/30	
Server		172.16.2.1/24	172.16.2.254
FW	E0/1	172.16.1.6/30	

(续)

设 备	端 口	IP 地址	网 关
FW	E0/2	10.10.10.5/30	
FW	E0/3	10.10.10.1/30	
FW	E0/4	172.16.2.254/24	
PC 1	F0/1	自动获取	自动获取
PC 2	F0/2	自动获取	自动获取
PC 3	无线连接	自动获取	自动获取
PC 4	F0/1	10.10.10.10/30	10.10.10.9/30
PC 5	F0/2	10.10.10.14/30	10.10.10.13/30



小贴士

- (1) 划分子网时应看清楚要求。
- (2) 数制转换应细心，转换后一定要对转换的结果进行检验。
- (3) IP 地址的使用以尽量节约为原则。

3. 任务要求

(1) 设定各设备的名称，交换机命名为“Switch-A”、“Switch-B”、“Switch-C”、“Switch-D”和“Switch-E”；路由器命名为“Router-A”和“Router-B”，防火墙命名为“FW”，无线接入点命名为“AP”。

(2) Router-A 设置 Telnet 登录，登录用户名为 teluser，密码为 admin。

(3) 为 5 台交换机的特权用户增加密码 super123，密码以加密方式存储。

(4) 手动配置三层交换机通过 22、23 号端口实现链路聚合。

(5) 在交换机上开启生成树协议。

(6) 在 Switch-A 和 Switch-B 上实现 HSRP，Switch-A 为 Master。

(7) 在 Switch-A 上实现 DHCP 协议，使得 PC1 和 PC2 能够自动获取地址等信息。

(8) 为 Switch-A 的端口 4 设定端口带宽限制，出入口均限速 1Mb/s。

(9) 在 Switch-B 的端口 8 上配置广播风暴抑制，允许通过的广播包数为 5000/s。

(10) 配置串口二层链路为 PPP 封装模式，采用 CHAP 认证方式实现双向认证，Router-A 上的用户名为 userB，密码为 shenzhou；Router-B 上的用户名为 userA，密码为 shenzhou。

(11) 西厂区的内部网络使用 RIP 路由协议，东厂区的内部网络使用 OSPF 路由协议，最终实现东西厂区之间的网络互连。

(12) 配置 Router-A，禁止 VLAN 20 访问互联网。

(13) 在 Router-A 和 Router-B 上分别建立 VPN 通道，要求使用 IPSec 协议的 ISAKMP 策略算法保护数据，配置预共享密钥，建立 IPSec 隧道的报文使用 MD5 加密，IPSec 变换集合定义为“ah-md5-hmas esp-3des”。两台路由器串口互连，Router-A 作为 DCE 端。

(14) 为保证内部网络安全，防止互联网的机器窥探内部网络，利用防火墙隐藏内部网络地址，使得外网用户不能直接访问园区网内的机器。

(15) 通过配置防火墙使内部地址能通过网络地址转换访问互联网。

(16) 在防火墙中使用合法 IP 地址 1.1.1.1 为 Server 配置 IP 地址映射，允许内网用户通过外网 IP 实现对该 Server 的 Web 访问。



（17）震荡波病毒常用的协议端口为 TCP 协议的 5544 和 445 端口，请配置三层交换机以防止病毒在局域网内肆虐。

（18）PC2 中已经搭建好 TFTP 服务，将所有网络设备的配置文件通过 TFTP 服务备份到 PC2 的 TFTP 服务器根目录中。

（19）通过对 AP 的配置，使公司没有有线网络的部分可以使用无线上网。

步骤实现

详细配置参见教学指导素材。

学习小结

本任务综合应用到了本书所学的安全知识，包括了计算机的安全接入、通过访问控制列表实现访问控制、设置网络设备权限、路由器的安全连接，以及网线制作等非本书的知识，必须熟练掌握这些知识点。通过本实训的训练，读者将进一步提高动手能力和综合素质。

反侵权盗版声明

电子工业出版社依法对本作品享有专有出版权。任何未经权利人书面许可，复制、销售或通过信息网络传播本作品的行为；歪曲、篡改、剽窃本作品的行为，均违反《中华人民共和国著作权法》，其行为人应承担相应的民事责任和行政责任，构成犯罪的，将被依法追究刑事责任。

为了维护市场秩序，保护权利人的合法权益，我社将依法查处和打击侵权盗版的单位和个人。欢迎社会各界人士积极举报侵权盗版行为，本社将奖励举报有功人员，并保证举报人的信息不被泄露。

举报电话：（010）88254396；（010）88258888

传 真：（010）88254397

E-mail: dbqq@phei.com.cn

通信地址：北京市万寿路 173 信箱

电子工业出版社总编办公室

邮 编：100036

